# Pervasive AuditMaster

---

## *User's Guide*

**Guide to Using AuditMaster**

Pervasive Software Inc.
12365 Riata Trace Parkway
Building B
Austin, TX 78727 USA

Telephone: 512 231 6000 or 800 287 4383
Fax: 512 231 6010
Email: info@pervasive.com
Web: http://www.pervasive.com

*disclaimer*

PERVASIVE SOFTWARE INC. LICENSES THE SOFTWARE AND DOCUMENTATION PRODUCT TO YOU OR YOUR COMPANY SOLELY ON AN "AS IS" BASIS AND SOLELY IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THE ACCOMPANYING LICENSE AGREEMENT. PERVASIVE SOFTWARE INC. MAKES NO OTHER WARRANTIES WHATSOEVER, EITHER EXPRESS OR IMPLIED, REGARDING THE SOFTWARE OR THE CONTENT OF THE DOCUMENTATION; PERVASIVE SOFTWARE INC. HEREBY EXPRESSLY STATES AND YOU OR YOUR COMPANY ACKNOWLEDGES THAT PERVASIVE SOFTWARE INC. DOES NOT MAKE ANY WARRANTIES, INCLUDING, FOR EXAMPLE, WITH RESPECT TO MERCHANTABILITY, TITLE, OR FITNESS FOR ANY PARTICULAR PURPOSE OR ARISING FROM COURSE OF DEALING OR USAGE OF TRADE, AMONG OTHERS.

*trademarks*

Btrieve, Client/Server in a Box, Pervasive, Pervasive Software, Pervasive AuditMaster, "know who's doing what to your data when, where and how," and the Pervasive Software and the Pervasive AuditMaster logos are trademarks or registered trademarks of Pervasive Software Inc.

Built on Pervasive Software, DataExchange, MicroKernel Database Engine, MicroKernel Database Architecture, Pervasive.SQL, Solution Network, Ultralight, and ZDBA are trademarks of Pervasive Software Inc.

Microsoft, MS-DOS, Windows, Windows 95, Windows 98, Windows NT, Windows Millennium, Windows 2000, Windows XP, Win32, Win32s, Windows 7, Windows 8, Windows Server 2008, Windows Server 2012, and Visual Basic are registered trademarks of Microsoft Corporation.

NetWare and Novell are registered trademarks of Novell, Inc.

NetWare Loadable Module, NLM, Novell DOS, Transaction Tracking System, and TTS are trademarks of Novell, Inc.

All other company and product names are the trademarks or registered trademarks of their respective companies.

© Copyright 2013 Pervasive Software Inc. All rights reserved. Reproduction, photocopying, or transmittal of this publication, or portions of this publication, is prohibited without the express prior written consent of the publisher.

This product includes software developed by KeyWorks Software. © Copyright 2002 KeyWorks Software. All rights reserved.

**Pervasive AuditMaster User's Guide**
**March 2013**
**100-004179-009**

# *Contents*


**1 Introducing Pervasive AuditMaster . . . . . 1-1**

*Understanding Pervasive AuditMaster and Its Capabilities*

What Is Pervasive AuditMaster? . . . . . 1-2
Features of Pervasive AuditMaster . . . . . 1-3
Pervasive AuditMaster Components . . . . . 1-4
Where to Go Next. . . . . 1-5

**2 Preparing to Install Pervasive AuditMaster. . . . . 2-1**

*Preparation Needed for Installation or Upgrade*

Installation Overview . . . . . 2-2
- Product Components . . . . . 2-2
- Utilities . . . . . 2-2
- Documentation. . . . . 2-3

Installation Checklists . . . . . 2-4
- Quick Checklist. . . . . 2-4
- Precautions . . . . . 2-4
- Permissions and Privileges . . . . . 2-5
- Authorization License . . . . . 2-5
- The Release Notes . . . . . 2-6

**3 Installing Pervasive AuditMaster . . . . . 3-1**

*Instructions for First-Time or Upgrade Installation*

Before You Begin . . . . . 3-2
- Installation Notes . . . . . 3-2
- Installation Notes for Windows Only . . . . . 3-3
- Upgrade Notes . . . . . 3-3

Installing Pervasive AuditMaster under Windows . . . . . 3-4
Installing AuditMaster Viewer as Client Only . . . . . 3-6
Common Questions After Installing Pervasive AuditMaster . . . . . 3-10
Uninstalling Pervasive AuditMaster . . . . . 3-11

**4 AuditMaster Basics . . . . . 4-1**

*An Overview of AuditMaster Basics*

Starting the AuditMaster Client . . . . . 4-2
Logging in from an AuditMaster Client . . . . . 4-3
Changing Your User Password. . . . . 4-4
Running AuditMaster under Pervasive PSQL Security . . . . . 4-5
Restarting the AuditMaster Event Handler . . . . . 4-11
Using Shortcut Menus . . . . . 4-12

**5 Using AuditMaster Viewer . . . . . 5-1**

*A Tour of the Main Window and a Reference List of Tasks*

AuditMaster Viewer Concepts . . . . . 5-2
AuditMaster Server . . . . . 5-2
Data Tree . . . . . 5-2
View File . . . . . 5-2
Alerts . . . . . 5-2
Reports . . . . . 5-2
AuditMaster Viewer GUI Visual Reference . . . . . 5-3
Title Bar . . . . . 5-4
Menu and Toolbar . . . . . 5-4
Data Tree. . . . . 5-7
Audit Record Grid. . . . . 5-7
Audit Record Detail . . . . . 5-7
Status Bar . . . . . 5-8

**6 Working with Audit Configurations . . . . . 6-1**

*How to Audit Data*

Configuring Data Monitoring without Schemas . . . . . 6-2
Configuring Data Monitoring with a Schema . . . . . 6-9
Operations to Audit by File . . . . . 6-16
Managing Schemas . . . . . 6-18
Importing a Schema from Pervasive PSQL . . . . . 6-19
Removing a Schema from AuditMaster . . . . . 6-23
Resolving Configuration Conflicts . . . . . 6-27

**7 Querying Audit Records . . . . . 7-1**

*How to Work with Audit Records*

Displaying Audit Records . . . . . 7-2
Working with the Audit Record Grid . . . . . 7-5
Audit Record Columns . . . . . 7-6
Viewing Audit Record Details . . . . . 7-7
Working with Archived Audit Records. . . . . 7-8
Using the Data Tree to Archive Audit Records . . . . . 7-9
Using Archive Manager . . . . . 7-11
Running Queries . . . . . 7-13
Displaying All Audit Records . . . . . 7-14
Restricting a Query . . . . . 7-14
Building an Advanced Query . . . . . 7-16
Using the Files Tab . . . . . 7-21
Running a Saved Query or Last Query Executed . . . . . 7-22
Working with Alerts . . . . . 7-24
Adding a New Alert . . . . . 7-25
Setting an Action for an Alert . . . . . 7-28

Editing an Existing Alert . . . . . 7-36
Stopping an Alert . . . . . 7-37
Printing Reports . . . . . 7-38
Searching Audit Records . . . . . 7-40
Sorting Audit Records . . . . . 7-42
Exporting Audit Records to Other Applications . . . . . 7-43
Displaying Audit Records under Pervasive PSQL Security . . . . . 7-44
Using AuditMaster Undo . . . . . 7-45

**8 Administering AuditMaster . . . . . 8-1**

*A Walk-through of Administrative Tasks*

Adding and Removing Servers . . . . . 8-2
Adding a Server . . . . . 8-2
Editing the Server Description . . . . . 8-5
Removing a Server . . . . . 8-5
Removing the Network Share . . . . . 8-6
Reviewing System Activity in the Status Log . . . . . 8-16
Maintaining Users . . . . . 8-18
Setting the Audit Filter . . . . . 8-20
Maintaining Server Settings . . . . . 8-22
Automated Archiving . . . . . 8-23
Archives to Keep . . . . . 8-24
Archive Disk Limit . . . . . 8-25
Errors to Audit . . . . . 8-26
Operations to Audit Globally . . . . . 8-27

**A Basic Troubleshooting . . . . . A-1**

*How to Identify and Solve Common Problems*

General Tips . . . . . A-2
Troubleshooting Strategies . . . . . A-3
Restarting the Status Log . . . . . A-4
Handling Errors Relating to Paths . . . . . A-5
No Records Returned by Query Despite Changes to Application Data . . . . . A-6
Network Communications . . . . . A-7
How to Start PSA . . . . . A-7
Documentation for PSA . . . . . A-7
Database Engine . . . . . A-8
How to Get Additional Help . . . . . A-9
Technical Support . . . . . A-10

**B Advanced Operations . . . . . B-1**

*Features for Power Users and Programmers*

Managing Schemas from the Command Line . . . . . B-2
import . . . . . B-3

export . . . . . B-4
remove . . . . . B-5
list. . . . . B-6
Querying Audit Data Directly through SQL . . . . . B-7
Query Data-Model Generator Utility . . . . . B-8
Creating a Virtual Database . . . . . B-9
The Structure of an Audit Record . . . . . B-12
Running a Query on the Current View File . . . . . B-15
Running a Query on an Archived File . . . . . B-17
Summary of Direct Query Methods . . . . . B-20
Using the Delta Alert Utility. . . . . B-22
Parameters for the amda Utility . . . . . B-23
Setting Delta Alert Email Recipients . . . . . B-24
Delta Alert Example. . . . . B-25

# *Figures*


1-1 AuditMaster monitors the database, not its front-end applications. . . . . 1-2
4-1 Server Configuration Shortcut Menu . . . . . 4-12
5-1 AuditMaster Viewer main window . . . . . 5-3
5-2 Menu and Toolbar . . . . . 5-4
5-3 Data Tree . . . . . 5-7
5-4 Audit Record Grid . . . . . 5-7
5-5 Audit Record Detail . . . . . 5-8
7-1 Query Builder . . . . . 7-3
7-2 Sample Audit Record Grid . . . . . 7-4
7-3 Query Builder Window . . . . . 7-13
7-4 Files Tab . . . . . 7-21
7-5 Structure of an Email Alert. . . . . 7-33
7-6 Edit Alert Window . . . . . 7-36
7-7 Report Builder after Running a Query and Selecting Audit Records . . . . . 7-38
B-1 Structure of a Delta Alert Email Message . . . . . B-29

# *Tables*


1-1 AuditMaster Components . . . . . 1-4
2-1 Pervasive AuditMaster Utilities . . . . . 2-2
4-1 Summary of AuditMaster Configurations under Pervasive PSQL Security Policies. . 4-5
5-1 Menu commands . . . . . 5-4
7-1 Visible Column Names in the Audit Data Grid . . . . . 7-6
7-2 Right-Click Commands for Archived Files in the Data Tree . . . . . 7-8
7-3 Options for Restricting a Query . . . . . 7-14
7-4 Saved Query Commands. . . . . 7-23
7-5 User and Database Names Audited under DefaultDB Database Security . . . . . 7-44
7-6 Results of Undo Command . . . . . 7-45
8-1 Default Errors to Audit after AuditMaster Installation . . . . . 8-26
A-1 UNC Path Settings for Remote AuditMaster Viewer Clients . . . . . A-5
A-2 Pervasive Software Resources . . . . . A-9
B-1 Audit Record Columns in a Virtual Database versus AuditMaster Viewer . . . . . B-13

# *About This Manual*

This manual introduces you to Pervasive AuditMaster, a security application for Pervasive PSQL Server. The book first leads you through preparation for installation or upgrade and installation and configuration steps.

The guide then explains how to work with the application. Topics include end-user and administrator tasks in Pervasive PSQL database environments both with and without Pervasive PSQL security enabled.

## Who Should Read This Manual

This manual provides information for both administrators and users who install and run the Pervasive AuditMaster system. It also includes a chapter on advanced operations for power users and developers of systems that use the audit data generated by AuditMaster.

## Manual Organization

This manual is divided into the following parts:

- Chapter 1—Introducing Pervasive AuditMaster provides background information on Pervasive AuditMaster and an overview of its data monitoring capabilities.
- Chapter 2—Preparing to Install Pervasive AuditMaster helps you prepare to install or upgrade your application.
- Chapter 3—Installing Pervasive AuditMaster provides the steps for first-time installation or upgrade of an existing installation.
- Chapter 4—AuditMaster Basics describes routine tasks you need to know how to do before using the application.
- Chapter 5—Using AuditMaster Viewer explains the user interface.
- Chapter 6—Working with Audit Configurations shows how to set up data monitoring.
- Chapter 7—Querying Audit Records offers a number of features for viewing and working with audit records.
- Chapter 8—Administering AuditMaster explains how to manage the auditing system.
- Chapter A—Basic Troubleshooting provides information for handling obstacles that may arise.
- Chapter B—Advanced Operations is for developers of applications that work with AuditMaster or that need direct access to audit records.

## *For More Information*

The following table lists resources for Pervasive AuditMaster and related software products:

| Product | Information Resources |
|---|---|
| Pervasive AuditMaster | • http://www.pervasive.com<br>• Pervasive AuditMaster User's Guide<br>• Pervasive AuditMaster online help |
| Pervasive PSQL | • http://www.pervasive.com<br>• Getting Started with Pervasive PSQL<br>• Pervasive PSQL User's Guide<br>• Pervasive PSQL SQL Language Reference<br>• Pervasive PSQL online help |

## Conventions

Unless otherwise noted, command syntax, code, and examples use the following conventions:

| | |
|---|---|
| CASE | Commands and reserved words typically appear in uppercase letters. Unless you are working with Linux or the manual states otherwise, you can enter these items using uppercase, lowercase, or both. For example, you can type `MYPROG`, `myprog`, or `MYprog`. |
| **Bold** | Words appearing in bold include the following: menu names, dialog box names, commands, options, buttons, statements, etc. |
| `Monospaced font` | Monospaced font is reserved for words you enter, such as command syntax. |
| [ ] | Square brackets enclose optional information, as in [*log_name*]. If information is not enclosed in square brackets, it is required. |
| \| | A vertical bar indicates a choice of information to enter, as in [*file name* \| @*file name*]. |
| < > | Angle brackets enclose multiple choices for a required item, as in `/D=<5\|6\|7>`. |
| *variable* | Words appearing in italics are variables that you must replace with appropriate values, as in *file name*. |
| … | An ellipsis following information indicates you can repeat the information more than one time, as in [*parameter*…]. |
| ::= | The symbol ::= means one item is defined in terms of another. For example, a::=b means the item *a* is defined in terms of *b*. |

chapter

# 1

# *Introducing Pervasive AuditMaster*

*Understanding Pervasive AuditMaster and Its Capabilities*

This chapter provides an overview of Pervasive AuditMaster and its features. It is divided into the following sections:


- What Is Pervasive AuditMaster?
- Features of Pervasive AuditMaster
- Pervasive AuditMaster Components
- Where to Go Next

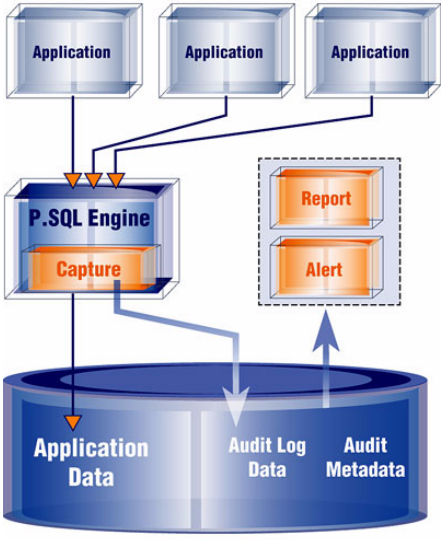
## What Is Pervasive AuditMaster?

AuditMaster is a transaction intelligence and monitoring product for organizations that need to track access to and change in their mission-critical data. AuditMaster provides a detailed audit trail. For every transaction affecting your database, you can quickly identify the following things:

- Who accessed a record or performed a change
- What change has taken place
- When the access or change occurred
- Where the access or change originated
- How the change was made

AuditMaster monitors databases, not client applications. It logs access to the database as well as changes made to data—including the reading of records, even if no change is made.

*Figure 1-1 AuditMaster monitors the database, not its front-end applications.*




AuditMaster creates a comprehensive audit trail. Every time a record changes, AuditMaster logs it both before and after the change, making it possible to recover from posting or data entry errors, because the log shows precisely who made what change when.

## Features of Pervasive AuditMaster

To provide a secure audit trail, AuditMaster includes the following features:

- A comprehensive logging system
  Captures the full range of events in your database and also stores database records before and after changes occur, whether from transactions by third-party applications or from direct changes to data
- A query builder
  A graphical interface for customizing queries and tracking errors
- Alerts
  Sends email to selected people or launches a selected application when defined events occur
- Reports
  Details the who, what, when, where, and how behind every transaction in a report either displayed on-screen or for hardcopy printing
- Archive manager
  Includes compression capability, for storage and retrieval of your historical information

## Pervasive AuditMaster Components

The following table shows the three main software components that work together in AuditMaster.

*Table 1-1 AuditMaster Components*

| Component | Description |
|---|---|
| Log event handler | Back-end component for monitoring and logging information about all database activity. The event handler runs on the database server at all times.<br><br>The Log event handler is avaiable for both 32 and 64-bit platforms. |
| Data definition files | Schema information required by the AuditMaster Viewer client to interpret readable data fields in monitored database records and to enable alerts set to specific fields within a record |
| Viewer | Front-end user interface for querying, presenting, and reporting database events logged by AuditMaster |

## Where to Go Next

The following topics may be of interest:

- To install the application, see Chapter 2: Preparing to Install Pervasive AuditMaster.
- To learn about basic operations, see Chapter 4: AuditMaster Basics.
- To find troubleshooting information, see Appendix A: Basic Troubleshooting.

chapter

# 2

# *Preparing to Install Pervasive AuditMaster*

*Preparation Needed for Installation or Upgrade*

This chapter contains the following topics:


- Installation Overview
- Installation Checklists

# Installation Overview

This section provides an quick summary of Pervasive AuditMaster product components, utilities, and documentation.

## Product Components

AuditMaster consists of the following product components:

- Event handler (32-bit and 64-bit versions available)
- Viewer client and utilities
- Data definition files
- Documentation

See What Is Pervasive AuditMaster? for an overview.

## Utilities

The AuditMaster Viewer client provides several utilities to control and manage audit activities. These are listed in the following table.

*Table 2-1 Pervasive AuditMaster Utilities*

| Utility | Use |
|---|---|
| Audit Configuration | Set up and manage data monitoring. See Chapter 6: Working with Audit Configurations. |
| Query Builder | Create, run, and save queries of audit records. See Chapter 7: Querying Audit Records. |
| Report Builder | Create, run, and save audit record reports. See Printing Reports. |
| Alerts | Create, save, and manage audit alerts (Windows only). See Working with Alerts. |
| Archive Manager | Manage audit record archives. See Maintaining Server Settings. |
| Schema Management Wizard | Import data definitions from database systems. See Managing Schemas. |
| Query Data Model Generator (QDMG) | Query audit record data through SQL. See Querying Audit Data Directly through SQL. |
| AuditMaster Delta Alerts (AMDA) | Configure alerts based on delta queries against audit data. See Using the Delta Alert Utility. |

### Documentation

Pervasive AuditMaster includes the *Pervasive AuditMaster User's Guide* as online help. The guide covers installation and use of the product. Access the online version or print the manual from the PDF file found on the CD-ROM or installed under the Docs folder.

## Installation Checklists

This section provides you with checklists and other information to prepare you for installation or upgrade. The following overview is intended to accompany the software and hardware requirements listed on the Pervasive Software web site for Pervasive AuditMaster.

### *Quick Checklist*

Each checklist item is described in detail in the topics that follow.

- ❑ You have taken the appropriate precautions before installing.
- ❑ Your system meets minimum hardware and software requirements.
- ❑ You have full administrator-level permissions and privileges on the machine where you plan to install AuditMaster.
- ❑ You have a license (unless you want a trial version).
- ❑ At the end of the installation, you have access to the latest release notes.

### *Precautions*

On Windows servers, the Pervasive PSQL database engine must be stopped and restarted during AuditMaster installation. If your business prohibits stopping the database during certain hours, install AuditMaster at an acceptable time.

Back up any important files on the target hard drive, including data files, before you proceed.

Before starting installation, disable any antivirus and antispyware applications. These may be reenabled immediately after installation is complete. If you do not disable antispyware, be prepared when prompted to allow various installation tasks to execute.

### *Permissions and Privileges*

To install Pervasive AuditMaster, you need the following:

- Full administrator-level rights on the machine where you are installing either AuditMaster or its viewer client
- Under Windows 2003, 2000, or XP, the File and Printer Sharing for Microsoft Networks component must be enabled in the Local Area Connection properties on the Pervasive PSQL server where AuditMaster is to monitor data.

### *Authorization License*

If you enter no license key during installation, you will be able to audit data for an evaluation trial period. At the end of that time, if you do not enter a license key, AuditMaster will cease to monitor data but will otherwise not interfere with your Pervasive PSQL system. After the trial period ends, you still will be able to query audit records captured during the trial, although certain features may no longer be available.

To apply a license key , you may open Pervasive PSQL Control Center and use select Tools ▸ License Administrator or open a command prompt and run clilcadm. For more information on license keys, see Pervasive PSQL *User's Guide*.

No license key is required for the AuditMaster Viewer remote client installation.

### *The Release Notes*

Pervasive Software urges you to read the release notes in the readme_am.htm file for product news that could not be included in the user documentation but may be essential to your successful installation and use of this product.

The readme_am.htm file is located under the root directory on the Pervasive AuditMaster CD-ROM as well as in the installation directory on the server after installation.

chapter

# 3

# *Installing Pervasive AuditMaster*

*Instructions for First-Time or Upgrade Installation*

This chapter explains how to install Pervasive AuditMaster either as an upgrade of an existing release or for the first time.

The following sections installation procedures:


- Before You Begin
- Installing Pervasive AuditMaster under Windows
- Installing AuditMaster Viewer as Client Only
- Common Questions After Installing Pervasive AuditMaster
- Uninstalling Pervasive AuditMaster

## Before You Begin

Familiarize yourself with this section to successfully install or upgrade Pervasive AuditMaster. Review the following:

- Preparing to Install Pervasive AuditMaster for needed information, including system requirements and platform-specific notes relevant to your operation.
- The Release Notes (readme_am.htm file) for important product news that could not be included in the product documentation but may be essential to your installation and use of the product release. The readme file is located at the root on the installation CD.

The rest of this section provides additional preinstall information:

- Installation Notes
- Upgrade Notes

### *Installation Notes*

Be aware of the following conditions before installing Pervasive AuditMaster on any platform.

- You must have full administrator-level rights on the machine where you install Pervasive AuditMaster.
- Disable any antivirus and antispyware applications. These may be reenabled immediately after installation is complete. If you do not disable antispyware, be prepared when prompted to allow various installation tasks to execute.
- On Windows servers, the Pervasive PSQL database engine is stopped and restarted during AuditMaster installation. If your business prohibits stopping the database during certain hours, install AuditMaster at an acceptable time.
- If you are installing an AuditMaster Viewer client to access a Pervasive PSQL system in which security is enabled and security policy is set to either Mixed or Database, see Running AuditMaster under Pervasive PSQL Security. Prepare to set up AuditMaster in a Pervasive Security environment by first familiarizing yourself with the security chapter in Pervasive PSQL *Advanced Operations Guide*. Note that for successful

installation when database security is enabled, the Prompt for Client Credentials setting must be selected in Pervasive PSQL Control Center (PCC) in the Properties ▸ Access window for the Pervasive PSQL engine.

- If the installation fails before the program copies any files to the target installation directory, refer to the installation log file (manifest.txt) in the AuditMaster installation directory.

### Installation Notes for Windows Only

On Microsoft Windows systems, be aware of the following conditions before installing Pervasive AuditMaster.

- When installed on a Pervasive PSQL server, the standard AuditMaster installation creates a hidden administrative share. When AuditMaster Viewer is installed as a remote client, access to that share is required. Before installing in either case, we recommend registering the share with any firewall system you may be running. By default, the share name is PVSWAUDIT$ for the path C:\<*installation directory*>\Audit, but both the name and path can be set to other values at installation time. Also, the share need not be hidden. To meet security requirements, the share can be replaced with an explicit local path name. For instructions, see Removing the Network Share.

### Upgrade Notes

The following notes pertain to upgrades from earlier versions.

- The upgrade from version 6.*x* to 6.4 can replace the existing AuditMaster installation without loss of audit records, server settings, users and passwords, saved queries, reports, or alerts.
- If you are upgrading from version 6.*x* to 6.4, to ensure a complete audit log, we recommend that you open the AuditMaster Viewer client on the server, update the current view file, and then archive it before installing the upgrade.
- For a server upgrade, all AuditMaster Viewer remote clients should be closed. For best results, also upgrade all AuditMaster Viewer clients on your network.

# Installing Pervasive AuditMaster under Windows

You must install AuditMaster on a machine with a Pervasive PSQL server engine.

This section guides you through the process of setting up Pervasive AuditMaster under Microsoft Windows. It provides instructions for running the Windows setup of the AuditMaster event handler and an AuditMaster viewer client on the Pervasive PSQL server machine where data will be monitored.

You must install Pervasive AuditMaster at the Pervasive PSQL server itself; you cannot install it remotely from a client machine.

A Pervasive AuditMaster license authorizes one server installation, but you may install as many viewer clients as needed across your network environment. For details, see Installing AuditMaster Viewer as Client Only.

### ➤ To run the Windows AuditMaster setup program

1 Log on to the machine as a Windows administrator.

Be sure that the machine meets the system requirements.

2 Launch the setup program from a Windows machine in one of the following ways:

| If using... | Do... |
|---|---|
| CD-ROM release | Insert the AuditMaster CD-ROM and allow it to start. If it does not do so automatically, open the file *drive*:\setup.exe (where *drive* is the drive letter of your CD-ROM). |
| Downloaded files | Open the file setup.exe in the download directory. |

The Welcome dialog box appears.

3 At the Welcome screen, click Next.

4 On the License Agreement page, read and accept the Software License Agreement, and then click Yes.

If upgrading, setup completes and skips to step 9.

5 Enter the license key provided with Pervasive AuditMaster and click Next.

**Note** Without a license, you can audit for the trial evaluation period. After that, auditing ends, but any logged audit records can be queried. For more information, see Authorization License.

6 If needed, change the default installation location to suit your local environment.

We recommend a location with at least 200 MB of storage space to allow for growth of audit records.

Click Next.

The setup installs needed files, then asks for a share name.

7 Accept the default share name PVSWAUDIT$ or enter an alternate share name, and click Next.

The setup summarizes the installation and asks you to confirm.

8 Do one of the following:

- Click Back to change the installation folder.
- Click Next to continue installing.

When you continue, setup installs needed files, then displays the AuditMaster Setup Complete window.

9 Select one of the following:

- To restart the machine on which you are installing AuditMaster, select Yes, I want to restart my computer now.

  AuditMaster will be unable to monitor data until you restart the machine.

- To restart your computer at a later time, select No, I will restart my computer later.

10 Click Finish.

The AuditMaster setup program restarts the machine if you chose to do so.

You have now successfully installed Pervasive AuditMaster.

The next task is to set up data monitoring, as described in Chapter 6: Working with Audit Configurations.

## Installing AuditMaster Viewer as Client Only

For Microsoft Windows servers, the Pervasive AuditMaster installation automatically places a viewer client on the same machine where the AuditMaster event handler and the Pervasive PSQL server reside. You may also manually install the viewer by itself on other machines in your network, which it will connect to the AuditMaster server as a remote client.

### ➤ To perform a client-only installation

1. Check for a Pervasive PSQL client on the machine where you wish to install the AuditMaster Viewer client.
2. Log on to the machine as a Windows administrator.
3. To access the client setup program, do one of the following:

| If using... | Do... |
|---|---|
| CD-ROM | In the client machine, insert the AuditMaster CD-ROM. If the Pervasive AuditMaster installation automatically starts, exit from the program, then open the file drive:\Client\setup.exe (where drive is the drive letter of your CD-ROM). |
| Files copied from an AuditMaster server | Copy the client installation folder (e.g., default location C:\<*installation directory*>\Audit\Client) from the server to the client machine and open the file \Client\setup.exe. |
| Downloaded files | Copy the client installation folder from the download directory to the client machine and open the file \Client\setup.exe. |

   The Welcome dialog box appears.

4. Read the Welcome text, and click Next.

   The Software License Agreement dialog box appears.

5. Read the license agreement. To accept the agreement, click Yes.

   No license key is required for client-only installation.

   The Choose Destination Location dialog box appears.

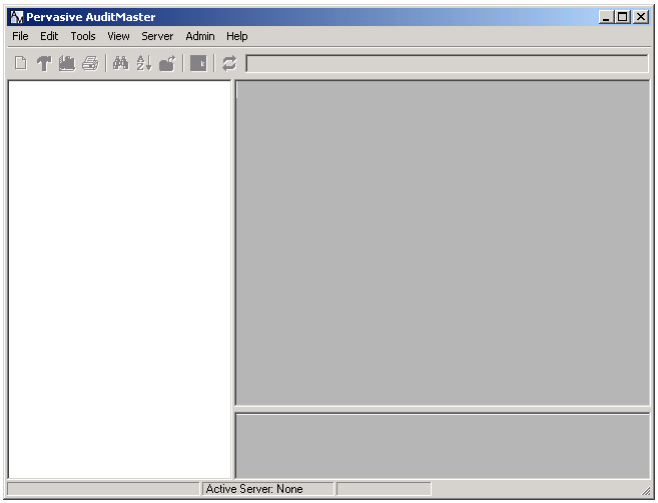
6. If needed, change the default installation location C:\<*installation directory*>\Audit to suit your local environment, and click Next.

The setup completes the installation of the AuditMaster Viewer client.

**7** Check the server machine you wish to add to make sure that Pervasive PSQL services are running. You may use Pervasive PSQL Control Center for this verification.

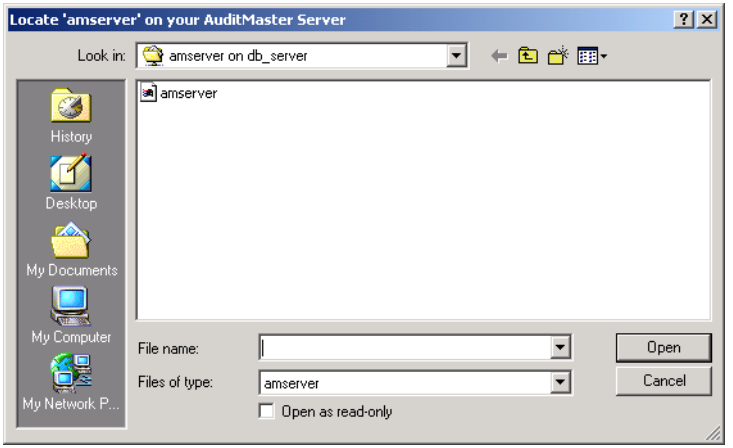
**8** To connect the new client to an AuditMaster server, open AuditMaster Viewer from the operating system Start menu or Start screen.

The Pervasive AuditMaster main window appears.




**9** Select Server ▸ Add.

The Locate 'amserver' on Your AuditMaster Server dialog box appears.

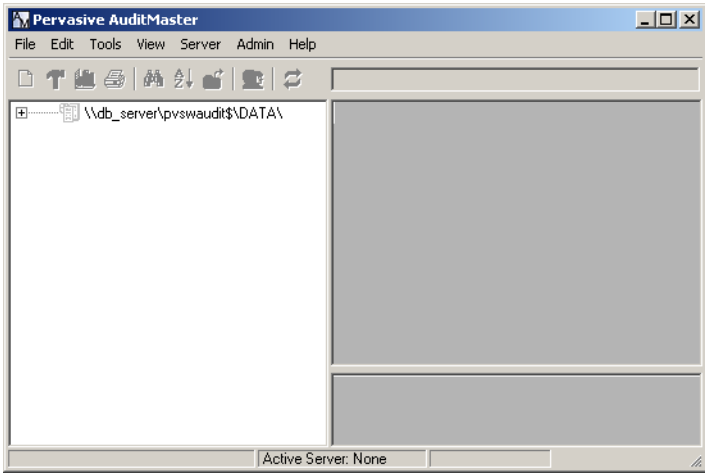



**10** Enter the path to the file amserver to read the settings for the AuditMaster server to which you want to a client connection.

- Windows default *server*\PVSWAUDIT$\DATA\amserver, where *server* is the name of the Pervasive PSQL machine with the database to be audited. Note that a share name other than PVSWAUDIT$ may have been chosen.

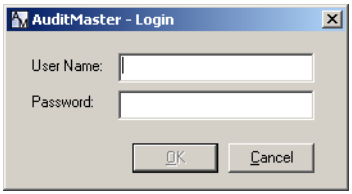
**11** Click Open.

The server you selected is added to the list.




**12** Right-click a server configuration and select Login. You may also double-click the configuration.

The AuditMaster Login dialog box appears.




**13** Enter a valid user name and password, and click OK to activate the command menus.

The Viewer client is now ready to use.

**Note** AuditMaster has a built-in user ID admin, for which the installation sets the default password MASTER. Passwords are case-sensitive, but user names are not. For security reasons, you will want to consider changing this password. Note that AuditMaster user accounts are unrelated to network, local, or database user logins. For remote client access to a Pervasive PSQL system with security policy is set to either Mixed or Database, follow the instructions under Running AuditMaster under Pervasive PSQL Security.

## Common Questions After Installing Pervasive AuditMaster

This section contains information that you may have after running the installation program.

### *Where are the AuditMaster release notes?*

The readme_am.htm file is located under the root directory on the Pervasive AuditMaster CD-ROM as well as in the installation directory on the server after installation.

### *Do I have to configure anything in Pervasive PSQL Control Center (PCC) for AuditMaster?*

No. AuditMaster requires no special settings in PCC.

### *Does the AuditMaster installation create any log files?*

Yes. See the file manifest.txt.

- In a default Windows installation, you will find this log under C:\Program Files\Pervasive Software\PSQL\Audit\Bin.

### *Does an upgrade retain AuditMaster data and settings? (Windows only)*

Yes. The upgrade installation is designed to preserve the following items in your existing AuditMaster 6.0 or 6.1 system:

- Audit records and archived files
- AuditMaster users and passwords
- Audit configurations
- Server settings
- Alerts
- Queries
- Reports
- Status log

# Uninstalling Pervasive AuditMaster

Uninstalling AuditMaster removes its components under the folder <*installation directory*>\Audit. Files in other locations are untouched.

**Note** If your business prohibits stopping the database during certain hours, be aware that on Windows servers, AuditMaster removal stops and restarts Pervasive PSQL services.

### ➤ To remove AuditMaster from Windows

Under Windows, AuditMaster can be uninstalled from the Add or Remove Programs window in the Control Panel.

1. Assess the operating system functionality to add or remove programs.
2. Select Pervasive AuditMaster in the list and remove it.
3. When prompted, you may restart your system.

**Note** Uninstalling AuditMaster leaves existing audit records intact, but you can no longer use them unless you configure another application to access AuditMaster archived files.

### ➤ To remove AuditMaster Viewer from a Windows client

Removing AuditMaster from a Windows client is the same as for a Windows server, except that you select Pervasive AuditMaster Viewer for removal.

chapter

# 4

# AuditMaster Basics

*An Overview of AuditMaster Basics*

This chapter explains the basics of AuditMaster use, covering the following topics:

- Starting the AuditMaster Client
- Logging in from an AuditMaster Client
- Changing Your User Password
- Running AuditMaster under Pervasive PSQL Security
- Restarting the AuditMaster Event Handler
- Using Shortcut Menus

## Starting the AuditMaster Client

AuditMaster Viewer is a client interface for querying, displaying, and reporting database transactions logged by the AuditMaster event handler.

### ➤ To start AuditMaster Viewer

Access AuditMaster Viewer from the operating system Start menu or Start screen.

Before you can use AuditMaster, you must log in. See Logging in from an AuditMaster Client.

# Logging in from an AuditMaster Client

AuditMaster requires a user account with name and password. The type of account determines access to AuditMaster menu commands.

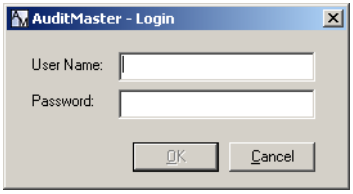
- User
  A regular user is able to query and view audit records and manage audit record archives.
- Administrator
  In addition to the above user privileges, an AuditMaster administrator can view the status log, set audit configurations, manage users, adjust system settings, and set the audit filter.

**Note** The built-in user ID admin has the default password MASTER. Passwords are case-sensitive; user names are not. To change this password, see Changing Your User Password. For information on the relation of AuditMaster logins to database and OS logins, read Displaying Audit Records under Pervasive PSQL Security.

### ➢ To log in to the viewer

1 In the data tree, right-click a server name to select Login, or double-click the server icon. To log in to the currently selected server, simply press Enter.

The login dialog box appears.




2 Enter a valid user name and password, and click OK.

You now have access to the server you selected.

**Note** For the AuditMaster server to recognize your login request, you need first to establish a regular network client login.

## Changing Your User Password

AuditMaster server access is password-protected. While logged in to a server, you can change your password for that server only. On other AuditMaster servers, your password may differ.

### ➤ To change your password

1 Log in to a server in the data tree.

2 Select Server ▸ Change Password.

The Change Password dialog box appears.

3 Enter your current password in the field provided.

4 Enter the new password in both fields provided.

The password is case-sensitive, can be up to 10 characters long, and may use any numbers or letters.

5 Click OK.

Your password is changed and must be used the next time you log in to AuditMaster.

**Note** The built-in user ID admin has the default password MASTER. Passwords are case-sensitive; user names are not. For information on the relation of AuditMaster logins to database and OS logins, read Displaying Audit Records under Pervasive PSQL Security.

# Running AuditMaster under Pervasive PSQL Security

You can run AuditMaster under the Pervasive PSQL database security features. We recommend you first familiarize yourself with the security chapter in the Pervasive PSQL *Advanced Operations Guide*.

AuditMaster installation under Pervasive PSQL security varies. Under Classic security policy, it does not differ from a standard installation. Under Mixed or Database policy, however, login authorization rights and storing of security credentials vary.

After installation, AuditMaster may require security configuration. The following table summarizes default configurations under the three Pervasive PSQL security policy settings. N/A means “not applicable.”

*Table 4-1 Summary of AuditMaster Configurations under Pervasive PSQL Security Policies*

| **Security Policy for DefaultDB** | Classic | Mixed | Database |
|---|---|---|---|
| **Security Enabled** | N/A | Yes | Yes |
| **Paths Entered in Data Locations for DefaultDB** | C:\<*installation directory*>\Samples<br>C:\<*installation directory*>\Audit (default)<br>(Entered but not used) | C:\<*installation directory*>\Samples<br>C:\<*installation directory*>\Audit (default)<br>Data and .ddf files | C:\<*installation directory*>\Samples<br>C:\<*installation directory*>\Audit (default)<br>Data and .ddf files |
| **OS Authentication** | OS or network login | OS or network login | N/A |
| **DB Authorization** | N/A | Database login | Database login |

*Table 4-1 Summary of AuditMaster Configurations under Pervasive PSQL Security Policies*

| **Security Policy for DefaultDB** | Classic | Mixed | Database |
|---|---|---|---|
| **Database Users** | N/A | Add AUDITUSERS group to DefaultDB with all database rights granted, then create AuditMaster users as members of the AuditMaster group.<br><br>Database user names and passwords **must match** OS or network logins exactly. | Add AUDITUSERS group to DefaultDB with all rights granted, then create AuditMaster users as members of the AuditMaster group.<br><br>Database user names and passwords **can differ** from OS or network logins, if they exist. |
| **Pervasive PSQL Security Configuration** | None required | See To configure Pervasive PSQL DefaultDB security for AuditMaster to run under Mixed or Database policy | See To configure Pervasive PSQL DefaultDB security for AuditMaster to run under Mixed or Database policy |

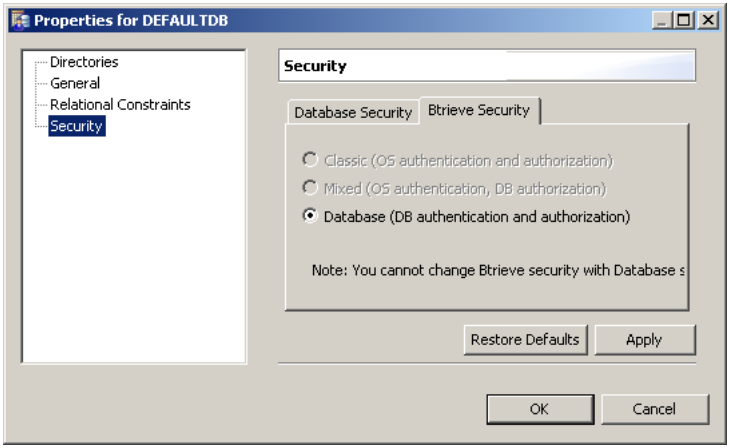
When the Pervasive PSQL DefaultDB security is enabled and security policy is set to Mixed or Database, the database engine must be configured in Pervasive PSQL Control Center (PCC) for AuditMaster to run. To do so, select Prompt for Client Credentials in the Properties ▸ Access window for the Pervasive PSQL engine.

### ➤ To configure Pervasive PSQL DefaultDB security for AuditMaster to run under Mixed or Database policy

1. Start Pervasive PSQL Control Center from the operating system Start menu or Start screen.
2. Use Pervasive PSQL Explorer to expand the Databases branch.
3. Right-click DefaultDB and select Properties.

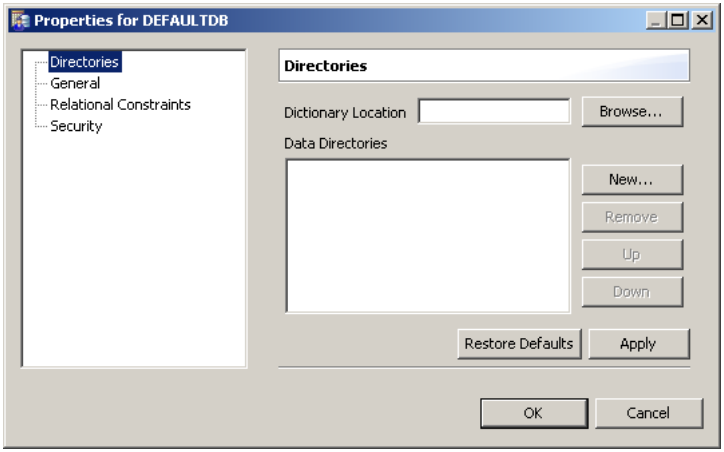
   The Properties window appears.
4. In the left-hand list, select Security.
5. In the right-hand pane, select Btrieve Security.

   The window displays Security settings (e.g., Database).




**6** In the left-hand list, select Directories.

The Directories window appears.



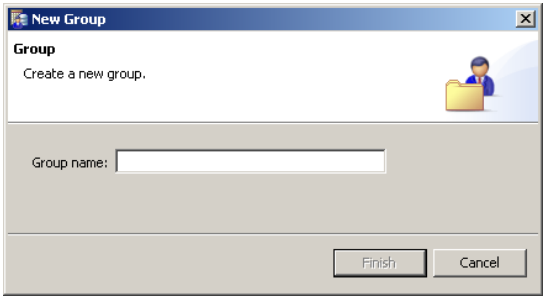

**7** Under Directories, use the New button to add the audited file path names.

Include all directories where application data files reside. If needed, contact the application vendor for file locations.

**8** When you're done, select OK to close the window.

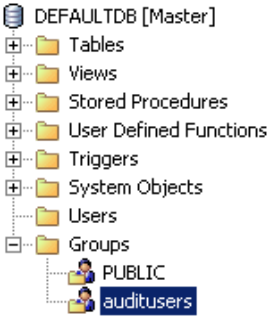
**9** In Pervasive PSQL Explorer under DefaultDB, right-click Groups ▸ New.

The New Group dialog box appears.



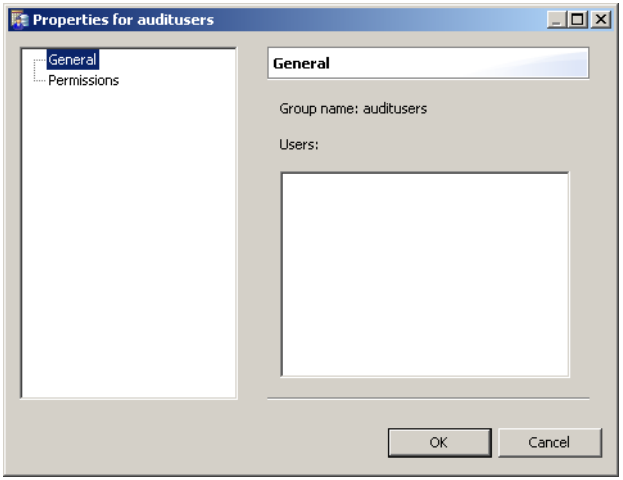

**10** In the Group Name field, enter auditusers, and click Finish.

The group auditusers appears in the DefaultDB branch under the Groups node, next to the built-in PUBLIC group.



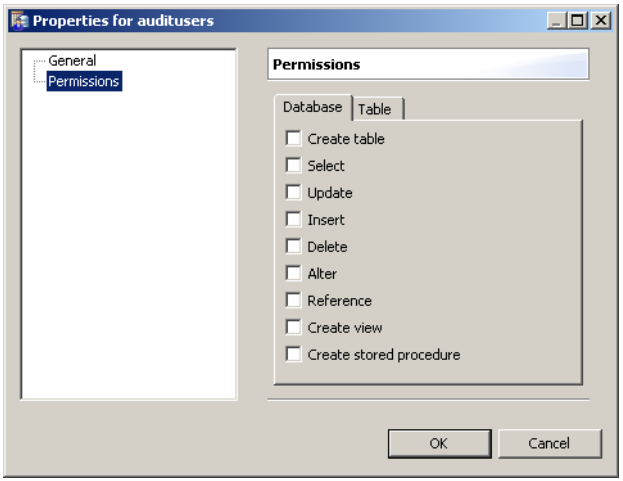

**11** Right-click auditusers ▸ Properties.

The group properties window appears.




**12** In the left-hand list, click Permissions.

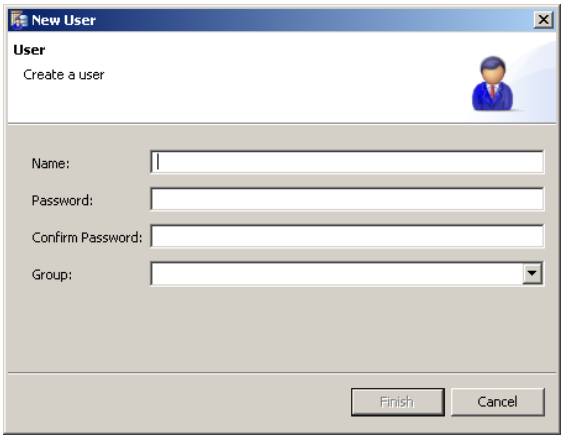
The group permissions for DefaultDB appear.




**13** Select checkboxes for all database rights, including Create Table, and click Close. No specific tables need be added to the list.

**14** In Pervasive PSQL Explorer under DefaultDB, right-click Users ▸ New ▸ User.

The New User window appears.




**15** Enter a user name and password for an AuditMaster user and select auditusers from the drop-down list. Note the following:

- Under Mixed security, a user name and password must match an OS login.
- Under Database security, a user name and password are unrelated to any OS login.

**16** Click Finish.

**17** Return to step 14 for to add other AuditMaster users as needed.

Once AuditMaster users are added, those with administrative rights within the AuditMaster application may begin to create audit configurations as described in Chapter 6: Working with Audit Configurations.

See also information under Displaying Audit Records under Pervasive PSQL Security.

**Caution** After enabling and configuring AuditMaster under Pervasive PSQL, if you need to change database security policy, first close all AuditMaster Viewer clients. Neglecting to do so will produce permission errors in the form of status code 94.

# Restarting the AuditMaster Event Handler

Most changes to AuditMaster configuration prompt you to restart the AuditMaster event handler before they take effect. Under Windows, viewer clients must not be running during this operation, or after the restart, network and database access errors will occur.

Depending on your platform, use one of the following methods:

- To restart the event handler under Windows

### ➢ To restart the event handler under Windows

1. Exit from all open instances of AuditMaster Viewer.
2. If Pervasive PSQL Control Center (PCC) is not running, start it from the operating system Start menu or Start screen.
3. In Pervasive PSQL Explorer, right-click the Services node and select Restart All Services.
4. Once services have restarted, you may reopen AuditMaster Viewer and continue data monitoring tasks.

## Using Shortcut Menus

Shortcut menus are an easy way to perform common tasks.

### ➤ To access a shortcut menu

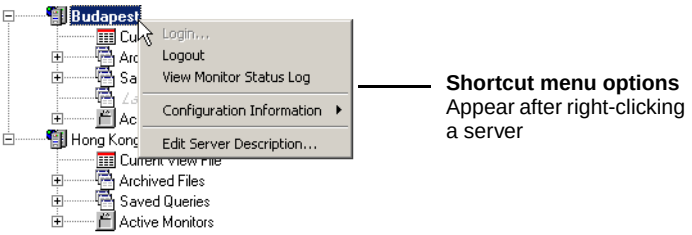
**1** Click an object in the viewer with your cursor.

The object is selected.

**2** On your mouse, click the right-most button.

A shortcut menu appears with a list of commands. The commands vary depending on the context. The following shortcut menu appears when you right-click a server in the data tree.

*Figure 4-1 Server Configuration Shortcut Menu*




**3** To perform a task from the shortcut menu, select an option from the menu.

The window for that task appears.

chapter

# Using AuditMaster Viewer

5

*A Tour of the Main Window and a Reference List of Tasks*

The topics in this chapter include:


- AuditMaster Viewer Concepts
- AuditMaster Viewer GUI Visual Reference

## AuditMaster Viewer Concepts

The viewer is a Microsoft Windows client user interface to the Pervasive AuditMaster system. From this main window, you may work with the following features:

- AuditMaster Server
- Data Tree
- View File
- Alerts
- Reports

### *AuditMaster Server*

An AuditMaster server is a Pervasive PSQL database server on which the Pervasive AuditMaster event handler and configuration files are installed and running. The event handler monitors the database and logs audit records which can then be queried for display in the AuditMaster Viewer client. Each AuditMaster server is a top branch in the AuditMaster data tree.

### *Data Tree*

The data tree presents your auditing system in graphical form. Each branch of the tree holds an AuditMaster server and its current view file, archived files, and saved queries. For more information, see AuditMaster Viewer GUI Visual Reference.

### *View File*

Audit records in an AuditMaster event handler log are moved to a view file for query and display. The records reside in the view file until they are moved to an archived file. Each server in the data tree has its own view file and archived files. For more information, see AuditMaster Viewer GUI Visual Reference.

### *Alerts*

An alert is an automated notification that a set of conditions has matched a newly captured audit record. A tripped alert can send email to a selected group of recipients. It also starts an application on the server. See Working with Alerts.

### *Reports*

Reports for viewing on-screen and printing are loaded with queries for selecting audit records. See Printing Reports.

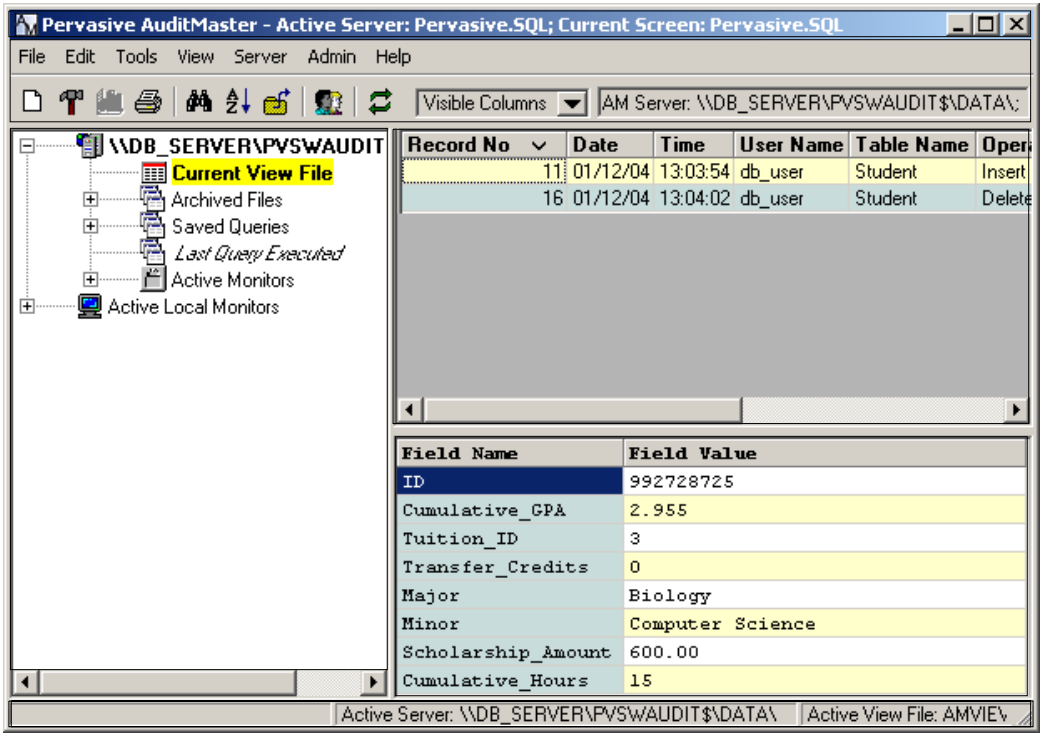
# AuditMaster Viewer GUI Visual Reference

This section provides a reference to main window of the AuditMaster Viewer graphical user interface (GUI). This window displays when the client application first starts. Once you have logged in as a user and run a query to display audit records, the GUI should resemble the following figure. The window includes the following objects:

- Title Bar
- Menu and Toolbar
- Data Tree
- Audit Record Grid
- Audit Record Detail
- Status Bar

For details, click any item in the list, or click an area of the image.

*Figure 5-1 AuditMaster Viewer main window*



## Title Bar

This section explains the title bar of the main window.

The title bar lists the name of the application, the active server, and the current screen. In this example, the system being monitored is a Pervasive PSQL database.

## Menu and Toolbar

This section describes items in the main window menu and toolbar, shown in the following figure. For details, click an area of the image.

*Figure 5-2 Menu and Toolbar*

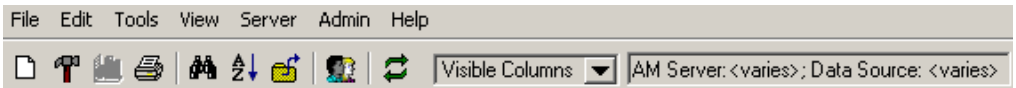



*Table 5-1 Menu commands*

| Menu or Toolbar | Command | Description |
|---|---|---|
| **File** | **Query** or | Displays the Query Builder to search for records. A query may be based on user, date, action, and other criteria. For details, see Chapter 7: Querying Audit Records. |
| | **Alert** or | Builds an alert based on a query (e.g., a certain user has made a change or when a check is cashed for over $100,000). A tripped alert flags the monitored record with an icon and performs an action, either sending email or starting a program. See details under Working with Alerts. |
| | **Report** or | Prints the selected audit records. See details under Printing Reports. |
| | **Exit** | Select **Exit** to log out and close the viewer |
| **Edit** | **Copy** | Copies selected fields to the clipboard as tab-delimited text strings |
| | **Select All** | Highlights all records |

*Table 5-1 Menu commands*

| Menu or Toolbar | Command | Description |
|---|---|---|
| **Tools** | **Search** or | Searches for specific text in audit records. For details, see Searching Audit Records. |
| | **Sort** or | Sorts audit records based on the currently selected column. For details, see Sorting Audit Records. |
| | **Export** or | Exports a current or archived view file to a text file. For details, see Exporting Audit Records to Other Applications. |
| **View** | **Show Active Local Monitors** | Displays an icon in the data tree to provide information about the currently installed event handler. The default for this setting is off and is left off under normal use. |
| | **Set Archives to Show** | Sets how many items are displayed under Archived Files in the data tree. For details, see Using the Data Tree to Archive Audit Records. |
| | **Show AM Debug Messages** | Sets whether debug messages are displayed in query results during certain integration development activities. The default for this setting is off and is left off under normal use. |
| | **Show AM Monitor Messages** | Sets whether internal messages are displayed in query results during certain integration development activities. The default for this setting is off and is left off under normal use. |

*Table 5-1 Menu commands*

| Menu or Toolbar | Command | Description |
|---|---|---|
| **Server** | **Add** | Creates a connection from an AuditMaster Viewer client to an AuditMaster server. |
| | **Remove** | Removes an AuditMaster server connection. The server continues to capture new audit records, but the client cannot currently access them, although it still can query and display records already in its current view and archived files. |
| | **Update Current View File** or | Refreshes the current view file from the audit log so that queries display the most up-to-date audit records. |
| | **Archive Current View File** | Archives all audit records in the current view file, including any captured in the log file but not yet updated to the view. |
| | **Archive and Compress View File** | Archives and compresses all audit records in the current view file, including any captured in the log file but not yet updated to the view. |
| | **Change Password** | Changes the password for the user currently logged into an AuditMaster server. |
| **Admin** (Available only to administrative logins.) | **View Status Log** | Displays the status log of Pervasive AuditMaster activity. |
| | **Audit Configuration** | Sets the files for an AuditMaster server to monitor, including any operations to be monitored for individual files. |
| | **User Maintenance** or | Allows you to add or remove users. |
| | **Server Settings** | Maintains paths and other system settings for an AuditMaster server. |
| **Help** | **Contents** | Provides an online version of the user's guide.. |
| | **Trouble-shooting** | Provides steps for troubleshooting common problems. For additional support, visit www.pervasive.com. |
| | **Index** | Displays the index of the user's guide. |
| | **About** | Displays Pervasive AuditMaster version information. |

*Table 5-1 Menu commands*

| Menu or Toolbar | Command | Description |
|---|---|---|
| **Visible Columns** | — | A drop-down list to set which columns display in the audit record grid. For steps, see Setting visible columns in the audit record grid. |
| **AM Server and Data Source** | — | The toolbar lists the current AuditMaster server login and the audit files selected for the last query, as shown in the following examples:<br>• AM Server: \\DB_SERVER\PVSWAUDIT$\DATA\<br>• Data Source: Current View File - \\DB_SERVER\PVSWAUDIT$\data\amview<br>• Data Source: Multiple View Files (i.e., both current view and archived files) |

## Data Tree

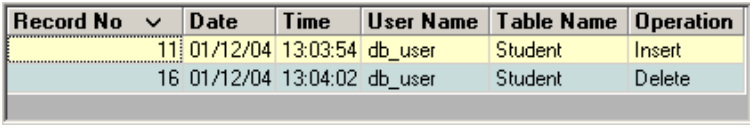
The data tree displays an AuditMaster server. Branches of the tree can be expanded by clicking the plus signs for more detail. You can also right-click tree icons for various command options. Queries may be run against the current view or archived files.

*Figure 5-3 Data Tree*

## Audit Record Grid

When a query is run against the current view or an archived file, the audit record grid shows the result.

*Figure 5-4 Audit Record Grid*



| Record No | Date | Time | User Name | Table Name | Operation |
|---|---|---|---|---|---|
| 11 | 01/12/04 | 13:03:54 | db_user | Student | Insert |
| 16 | 01/12/04 | 13:04:02 | db_user | Student | Delete |

## Audit Record Detail

Audit records capture both AuditMaster operations and database activity. For database activity, the audit record detail area in the lower

part of the AuditMaster Viewer window shows the fields of the data record where activity occurred.

*Figure 5-5 Audit Record Detail*

| Field Name | Field Value |
|---|---|
| ID | 992728725 |
| Cumulative_GPA | 2.955 |
| Tuition_ID | 3 |
| Transfer_Credits | 0 |
| Major | Biology |
| Minor | Computer Science |
| Scholarship_Amount | 600.00 |
| Cumulative_Hours | 15 |

**Note** Data record detail may be in human language or in hexadecimal, depending on whether the database schema has been imported for AuditMaster to use in displaying data. For more information, see Working with Audit Configurations.

## Status Bar

This section explains the text in the status bar at the bottom of the main window.

The status bar displays two messages during AuditMaster Viewer operation:

- The active server to which the viewer is currently a client, typically the following string:

  Active Server: *server_name*\PVSWAUDIT$\DATA\

- The active view file, typically the following string:

  Active View File: \AMVIEW.

chapter

# 6

# Working with Audit Configurations

*How to Audit Data*

The running of AuditMaster depends on audit configurations. An audit configuration combines three types of information:

- A Pervasive PSQL database server
- A list of files to monitor
- A schema imported from a Pervasive PSQL database (optional)

Schemas are not required to use AuditMaster, but they make audit records human-readable and enable more precise alerts.

Files monitored under an audit configuration may be arranged into groups. For example, if you have a different group of files for each customer in your application, you can give each customer's data files their own AuditMaster group. Groups are for organizing your thinking about auditing and have no affect on the operation of the AuditMaster system.

All groups under a single audit configuration must use the same schema. Also, only one schema can be used in each audit configuration. So, if you want to monitor a database using a different schema, you will create a separate audit configuration for that combination. Each file to be monitored can belong to only one group in one audit configuration.

We recommend you work through the following tutorials before attempting to create an audit configuration:

1. Configuring Data Monitoring without Schemas
2. Configuring Data Monitoring with a Schema
3. Operations to Audit by File
4. Managing Schemas
5. Resolving Configuration Conflicts

## Configuring Data Monitoring without Schemas

The tutorial in this section shows how to use an audit configuration consisting of the following:

- A Pervasive PSQL database server
- A group of database files for a fictional video store
- No schema (data dictionary files, or DDFs)

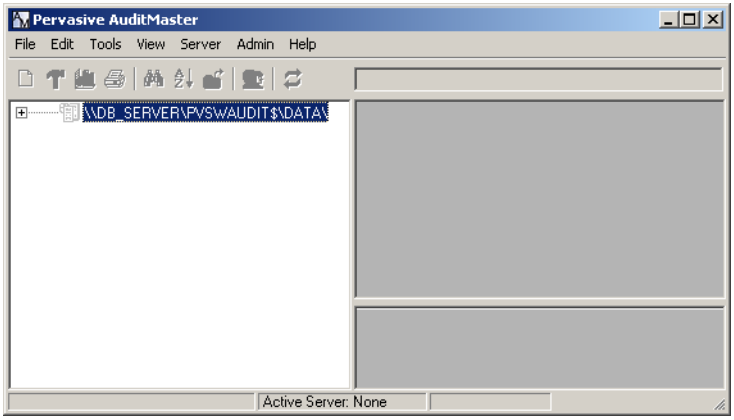
Only AuditMaster administrative users can set audit configurations.

The database used in this example is fictional. Simply read through the steps to become familiar with the audit configuration procedure. In the next tutorial, Configuring Data Monitoring with a Schema, you will have sample files for hands-on practice.

### ➤ To use an audit configuration without schemas

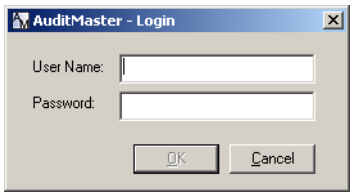
1 Open AuditMaster Viewer from the operating system Start menu or Start screen.

The Pervasive AuditMaster window appears. For Pervasive PSQL under Windows, an entry for the AuditMaster server was added by default during installation.



**2** Right-click the server to select Login. You may also double-click.

The AuditMaster Login dialog box appears.



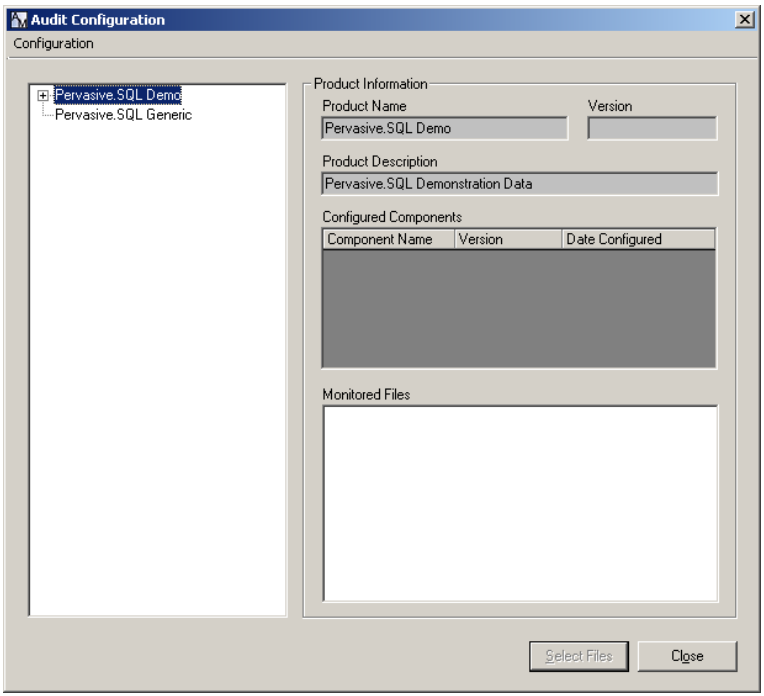

**3** Enter the default user name admin and the password MASTER.

**Note** The built-in user ID admin has the default password MASTER. Passwords are case-sensitive; user names are not.

**4** Click OK.

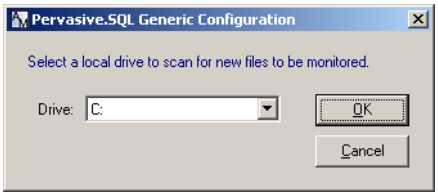
**5** Select Admin ▸ Audit Configuration.

The Audit Configuration window opens.



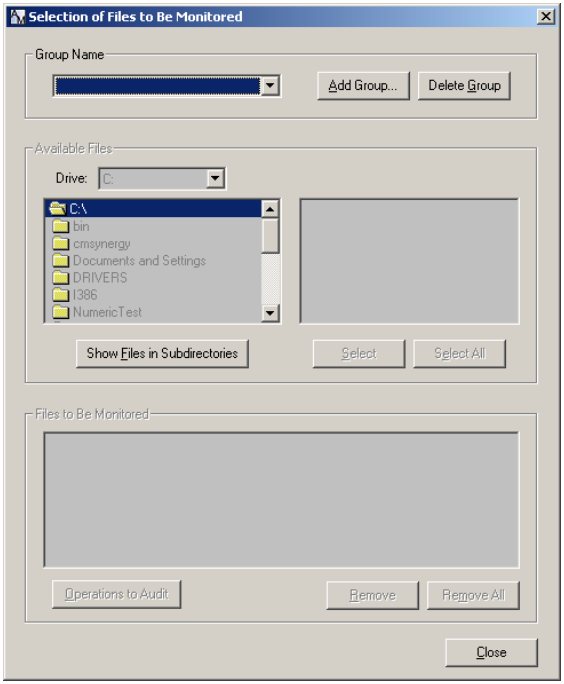
**6** In the left pane, right-click Pervasive PSQL Generic and select New Configuration. You may also double-click to open it.

The Pervasive SQL Generic Configuration dialog box appears:



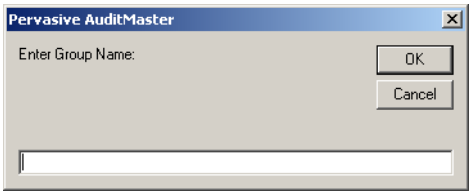

**7** From the drop-down list, select the drive on which to choose Pervasive PSQL data files to be monitored, and click OK.

The system displays the Selection of Files to Be Monitored window.



**8** Click Add Group.

The Enter Group Name dialog box appears.

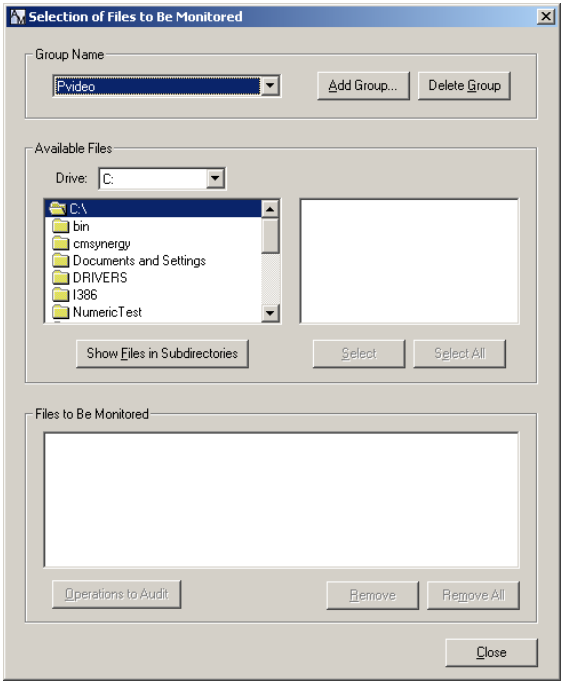



A group is a set of one or more files to monitor. Group names are case-sensitive and can use any keyboard characters, including spaces, up to 40 characters in length. Since group names are globally visible, it is recommended that you name a group to reflect the audit configuration under which you are creating it.

**9** Enter a group name, and click OK.

For this example, the group name Pvideo is used.

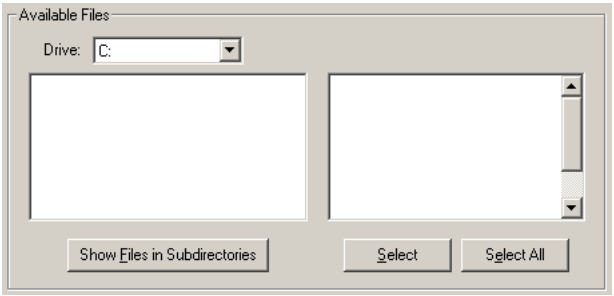
The Selection of Files to Be Monitored window activates the Available Files area.



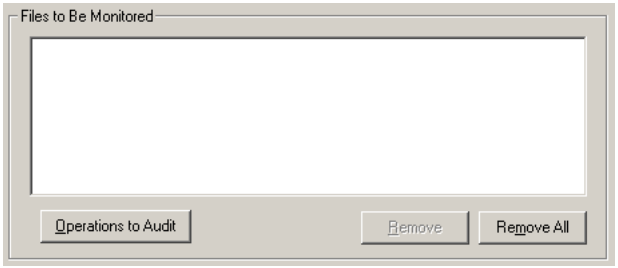
**10** In the Available Files area, navigate through the folder hierarchy to locate files to monitor. Only files in Btrieve format will be listed. You may also use the Show Files in Subdirectories button, after double-clicking a folder, to display a list of all Btrieve files from the double-clicked directory downward.

**Note** A large number of files may take time to display in the list.

**11** Highlight a file name, and click Select. You may also double-click to select a file.




The file path name appears in the Files to Be Monitored list.



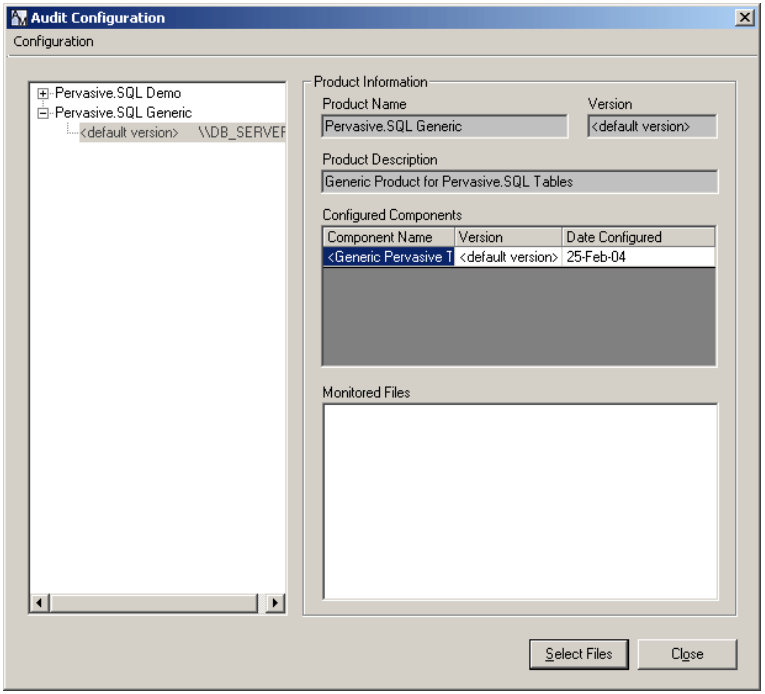

You can also click Select All to select every file in the current list.

If you decide not to monitor a file, select it and click Remove to delete it from the group. Remove All deletes all files from the group.

**Note** The Operations to Audit button enables you to override the global auditing settings applied to each selected file by default. See details under Operations to Audit by File.

**12** When you are finished, click Close.

In the Audit Configuration window, the Configured Components area identifies the new configuration for the product definition. Expanding the newly added group in the Monitored Files area lists the file that was added to the group.



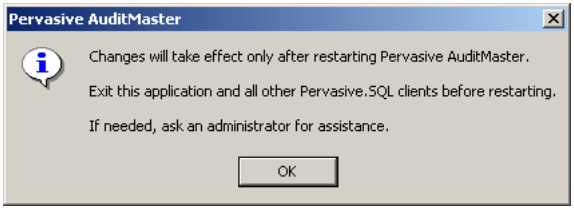

AuditMaster is now set to monitor the Pervasive PSQL file. The file and its group are associated only with this particular audit configuration.

**13** If you wish to change the audit configuration, do the following:

In the audit configurations, expand the one that contains the group and file you want to change, then click the Select Files button to display the Selection of Files to Be Monitored window and return to step 10.

**14** When you are finished with entries in the Audit Configuration window, click Close.

The window closes and the system prompts you to restart the AuditMaster event handler.


Pervasive AuditMaster
Changes will take effect only after restarting Pervasive AuditMaster.
Exit this application and all other Pervasive.SQL clients before restarting.
If needed, ask an administrator for assistance.
OK

**15** Click OK.

**16** Follow the steps given under Restarting the AuditMaster Event Handler.

After the restart, the new AuditMaster configuration becomes active and auditing begins.

# Configuring Data Monitoring with a Schema

The tutorial in this section shows how to set an audit configuration for the following:

- A Pervasive PSQL database server
- A demonstration database
- Demonstration database schema (data dictionary files, DDFs)

Schemas are not required to use AuditMaster, but they make audit records human-readable and enable more precise alerts.

Only AuditMaster administrative users can set audit configurations.

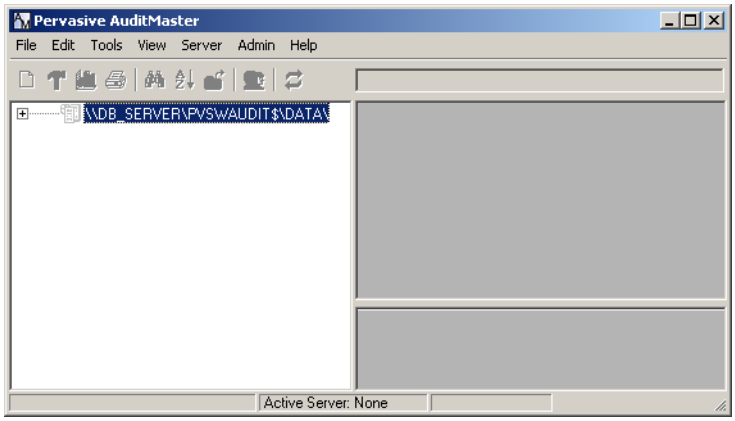
Your Pervasive PSQL installation includes a database for demonstration purposes, stored in the folder Demodata. For this tutorial, the schema for these tables has already been imported into AuditMaster so that you can experiment with audit records for the demonstration database.

Managing Schemas shows how to create a new audit configuration that uses your own application and its schema.

### ➢ To use an audit configuration with a schema

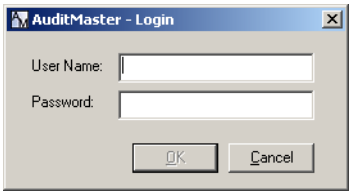
1 Open AuditMaster Viewer from the operating system Start menu or Start screen.

The Pervasive AuditMaster window appears, showing the server available.



**2** Right-click the server to select Login. You may also double-click.

The AuditMaster Login dialog box appears.



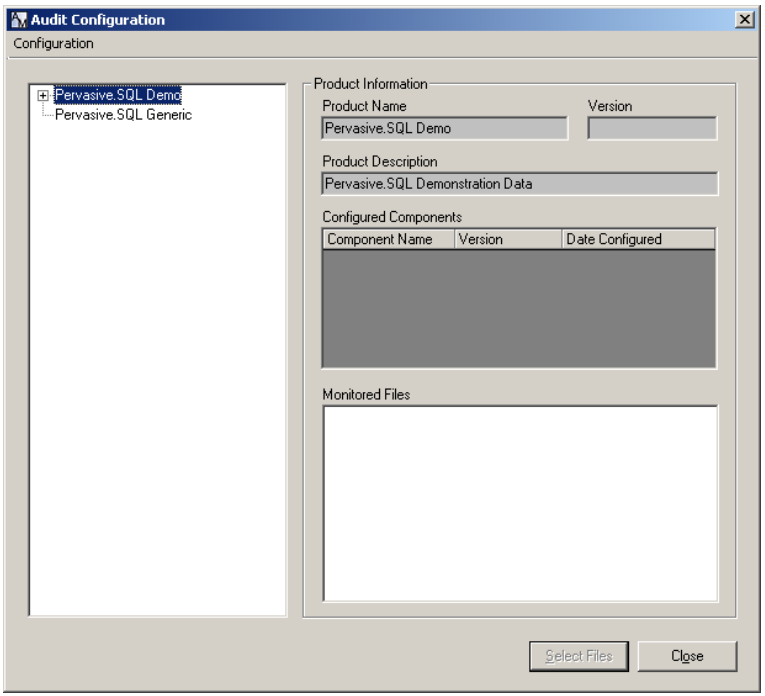

**3** Enter the default user name admin and the password MASTER.

**Note** The built-in user ID admin has the default password MASTER. Passwords are case-sensitive; user names are not.

**4** Click OK.

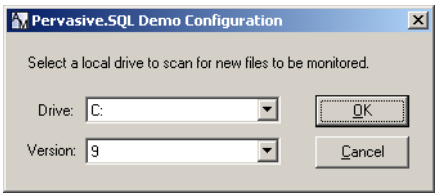
**5** Select Admin ▸ Audit Configuration.

The Audit Configuration window opens.



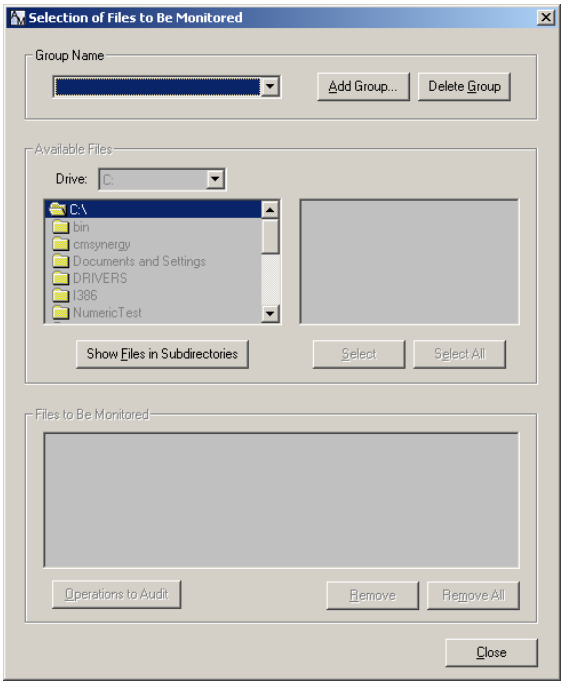
**6** In the left pane of the Audit Configuration window, right-click Pervasive PSQL Demo and select New Configuration. You may also double-click to open it.

The Pervasive PSQL Demo Configuration dialog box appears:



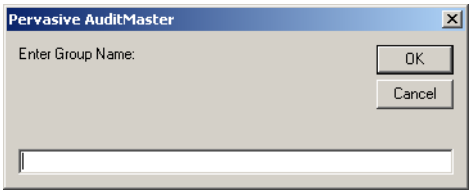

**7** If you have a standard Pervasive PSQL installation, click OK to accept the default drive C: for the Pervasive PSQL Demo drive location and the version of Pervasive PSQL. Otherwise, use the drop-down list to change to the appropriate location for your Pervasive PSQL database.

The system displays the Selection of Files to Be Monitored window.




**8** Click Add Group.

The Enter Group Name dialog box appears.



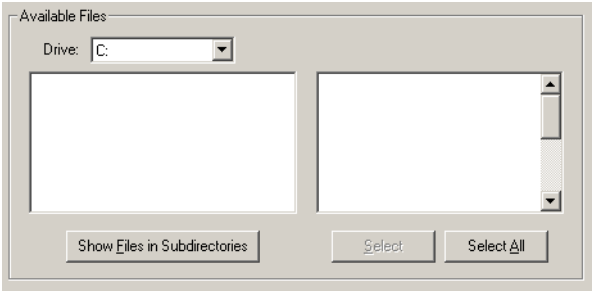

A group is a set of one or more files to monitor. Group names are case-sensitive and can use any keyboard characters, including spaces, up to 40 characters in length. Since group names are globally visible, it is recommended that you name a group to reflect the audit configuration under which you are creating it.

**9** Enter the group name Demodata, and click OK.

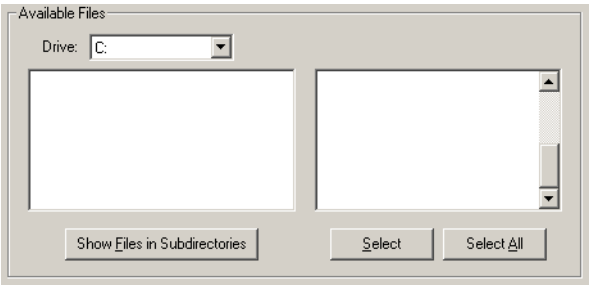
**10** In the Available Files area, navigate through the folder hierarchy to locate files to monitor. Only files in Btrieve format are listed. You may also use the Show Files in Subdirectories button, after double-clicking a folder, to display a list of all Btrieve files from the double-clicked directory downward.

**Note** Listing many folders and files may take several minutes.

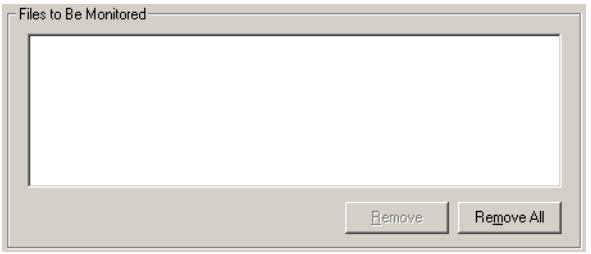
For this example, select the Pervasive PSQL demonstration directory C:\<*installation directory*>\Demodata.



**11** Click the file name student.mkd, and click Select. You may also double-click it.




The file path name appears in the Files to Be Monitored list.



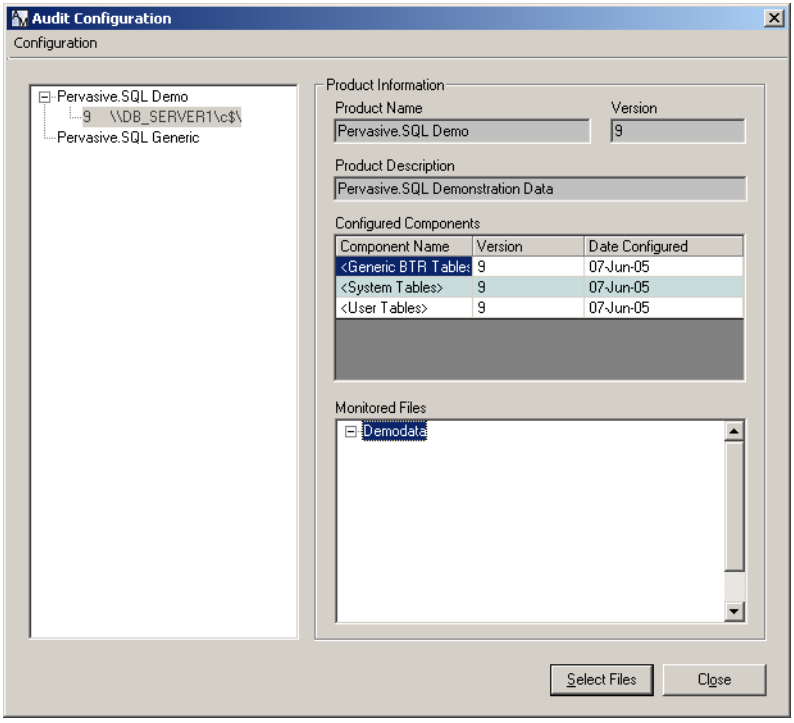

You can also click Select All to add every file in the current list.

Each file can be a member of only one group in one audit configuration. If you select a file that is already listed in another group, AuditMaster informs you of a configuration conflict. Should this occur, see Resolving Configuration Conflicts.

If you decide not to monitor a file, select it and click Remove to delete it from the group. Remove All deletes all files from the group.

**12** When you are finished selecting files, click Close.

In the Audit Configuration window, the Configured Components area identifies the new configuration. Expanding the newly added group in the Monitored Files area lists the files.




AuditMaster is now set to monitor the file.

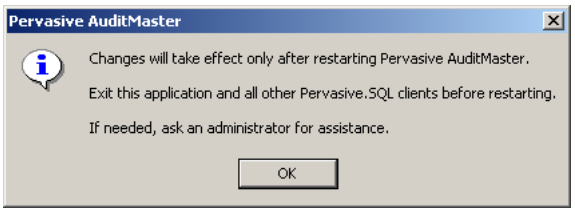
**13** If you wish to change the audit configuration, do the following:

In the audit configurations, expand the one that contains the group and file you want to change, then click the Select Files button to display the Selection of Files to Be Monitored window and return to step 10.

**Note** All groups and files in an audit configuration that uses a schema must use the same one. If you try to add a file that does not match the schema for the audit configuration, AuditMaster warns that the file is “not registered for monitoring.”

14 When you are finished with entries in the Audit Configuration window, click Close.

The window closes and the system prompts you to restart the AuditMaster event handler.


Pervasive AuditMaster
Changes will take effect only after restarting Pervasive AuditMaster.
Exit this application and all other Pervasive.SQL clients before restarting.
If needed, ask an administrator for assistance.
OK

15 Click OK.

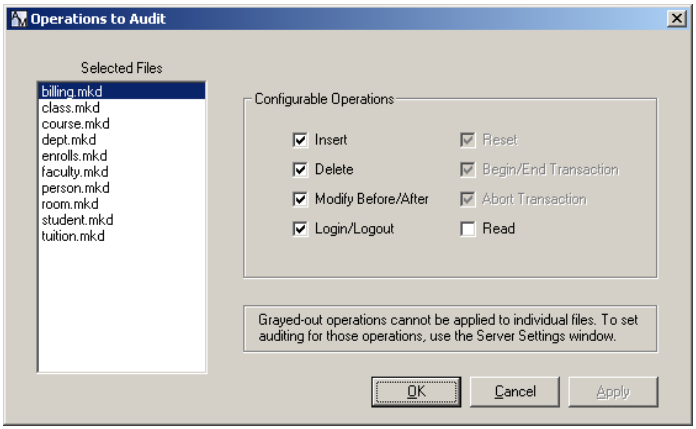
16 Follow the steps given under Restarting the AuditMaster Event Handler.

After the restart, the new AuditMaster configuration becomes active and auditing begins.

You are now ready to attempt to create an audit configuration for your own Pervasive PSQL database server, application, database files, and schema. Proceed to Managing Schemas.

## Operations to Audit by File

Each file in an audit configuration receives a default list of audit events, but you also can click the Operations to Audit button in the Selection of Files to Be Monitored window to reset that list as shown here.




The following table lists operations you can set for individual files. As with other new settings, you must restart the event handler.

| Operations to Audit by File | Default |
|---|---|
| Insert | On |
| Delete | On |
| Modify Before/After | On |
| Login/Logout | On |
| Reset | N/A |
| Begin/End Transaction | N/A |
| Abort Transaction | N/A |
| Read | Off |

See also Operations to Audit Globally.

**Note** In a Pervasive PSQL database, when the client-side cache engine is turned on, the cache engine reads an entire database page after 8 consecutive reads in anticipation of more reads. The records in the database page read by the cache engine are not audited by the event handler on the server. If auditing requires that every read be captured, verify the setting is off. However, lack of engine caching can reduce database performance. The behavior occurs only when the threshold of 8 consecutive reads is reached. If 7 reads and then an update occurs, no caching occurs and all 7 reads are captured. In Pervasive PSQL Control Center, expand Local Client, right-click MicroKernel Router, and select Properties, then click Performance tuning to see the setting Use Cache Engine. By default, the setting is off.

## Managing Schemas

AuditMaster can import Pervasive PSQL schemas for two purposes:

- To make data records more readable
- To enable alerts based on changes to a specific record field

Without its schema, application data in audit records appears as hexadecimal rows and you cannot set alerts for individual data fields. The example Configuring Data Monitoring without Schemas monitored files in a fictional video store database. Lacking a schema, the application data record for an insert resembled the following:

| Offset | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | [0123456789ABCDEF] |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00000000 | 07 | 00 | 00 | 00 | 41 | 75 | 62 | 65 | 72 | 6f | 6e | 20 | 20 | 20 | 20 | 20 | [þþþþAuberon ] |
| 00000010 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 52 | 65 | 79 | 20 | [ Rey ] |
| 00000020 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | [ ] |
| 00000030 | 20 | 20 | 20 | 20 | 39 | 30 | 32 | 31 | 20 | 53 | 70 | 61 | 6e | 73 | 6f | 72 | [ 9021 Spansor] |
| 00000040 | 20 | 52 | 64 | 2e | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | [ Rd. ] |
| 00000050 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | [ þþþþþþþþ] |
| 00000060 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | [þþþþþþþþþþþþþþþþ] |
| 00000070 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 41 | 75 | 73 | [þþþþþþþþþþþþþþAus] |
| 00000080 | 74 | 69 | 6e | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | [tin ] |
| 00000090 | 20 | 20 | 20 | 20 | 20 | 54 | 58 | 37 | 38 | 37 | 30 | 37 | 20 | 20 | 20 | 20 | [ TX78707 ] |
| 000000a0 | 20 | 35 | 31 | 32 | 2d | 35 | 35 | 35 | 2d | 32 | 33 | 30 | 32 | 01 | 00 | 00 | [ 512-555-2302þþ] |

After schema import, AuditMaster can better display the next insert:

| Field Name | Field Value |
|---|---|
| CustID | 7 |
| LastName | Auberon |
| FirstName | Rey |
| Address1 | 9021 Spansor Rd. |
| Address2 | |
| City | Austin |
| State | TX |
| Zip | 78707 |
| HomePhone | 512-555-2302 |

**Note** Schema import has no effect on display of data already captured.

The rest of this section covers the following topics:

- Importing a Schema from Pervasive PSQL
- Removing a Schema from AuditMaster

## *Importing a Schema from Pervasive PSQL*

The following example steps you through using the AuditMaster Schema Maintenance Wizard to import a schema from a Pervasive PSQL database. It uses the same fictional video store as in the previous example, and while no files are provided for hands-on practice, after reviewing the steps you should be ready to export a schema from your own application.

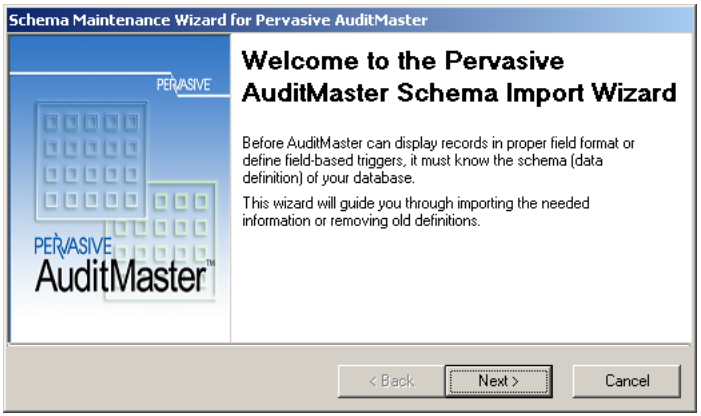
A command-line version of the wizard is described under Managing Schemas from the Command Line.

**Note** If you have set Pervasive PSQL security policy on the DefaultDB database to Mixed or Database, then before working with a new schema for an audit configuration, you must first add its path to the list of data locations for DefaultDB. See details under Running AuditMaster under Pervasive PSQL Security.

### ➢ To import a schema from a Pervasive PSQL database

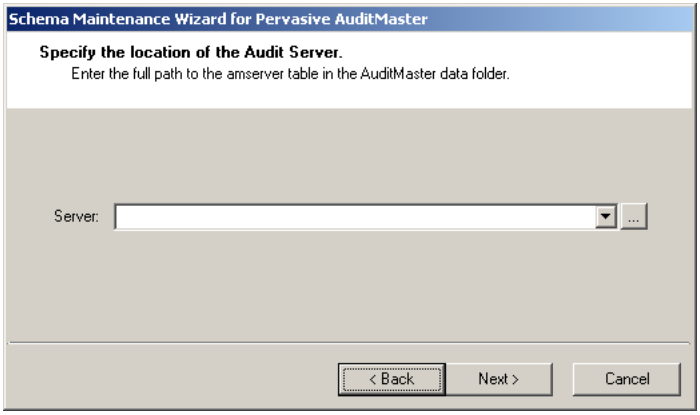
1 Access Schema Maintenance Wizard from the operating system Start menu or Apps screen.

The Schema Maintenance Wizard appears.


Schema Maintenance Wizard for Pervasive AuditMaster
PERVASIVE
PERVASIVE
AuditMaster
Welcome to the Pervasive AuditMaster Schema Import Wizard
Before AuditMaster can display records in proper field format or define field-based triggers, it must know the schema (data definition) of your database.
This wizard will guide you through importing the needed information or removing old definitions.
< Back
Next >
Cancel

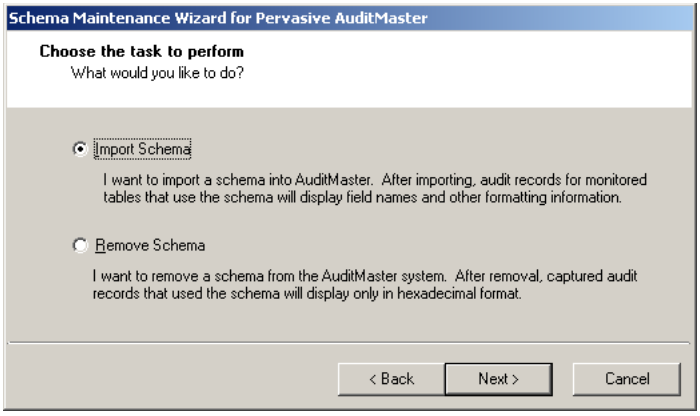
**2** Click Next to continue.

The wizard asks you to specify the location of the amserver file.


Schema Maintenance Wizard for Pervasive AuditMaster
Specify the location of the Audit Server.
Enter the full path to the amserver table in the AuditMaster data folder.
Server:
< Back
Next >
Cancel

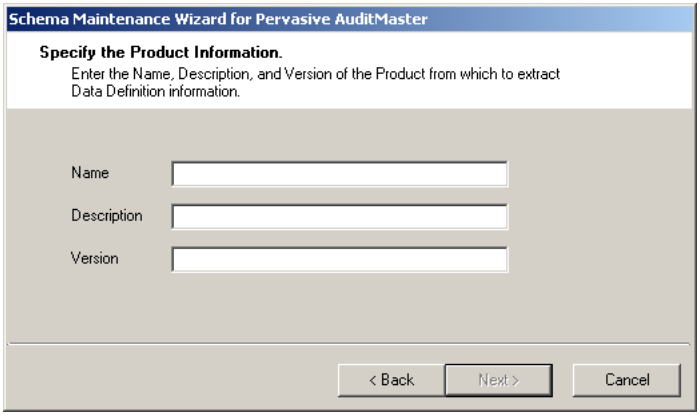
**3** Accept the default path to the file, or enter a custom path, and click Next. You may also use the ellipsis button to browse to a folder or network location.

The wizard asks you to choose to import or remove a schema.


Schema Maintenance Wizard for Pervasive AuditMaster
Choose the task to perform
What would you like to do?
Import Schema
I want to import a schema into AuditMaster. After importing, audit records for monitored tables that use the schema will display field names and other formatting information.
Remove Schema
I want to remove a schema from the AuditMaster system. After removal, captured audit records that used the schema will display only in hexadecimal format.
< Back
Next >
Cancel

**4** Select Import Schema and click Next.

The wizard asks you to enter information about the database application to be audited.


Schema Maintenance Wizard for Pervasive AuditMaster
Specify the Product Information.
Enter the Name, Description, and Version of the Product from which to extract Data Definition information.
Name
Description
Version
< Back
Next >
Cancel

5 Enter a name for the audit configuration.

You will use this name to identify the audited application in the Audit Configuration window.

6 Enter a description for the audit configuration.

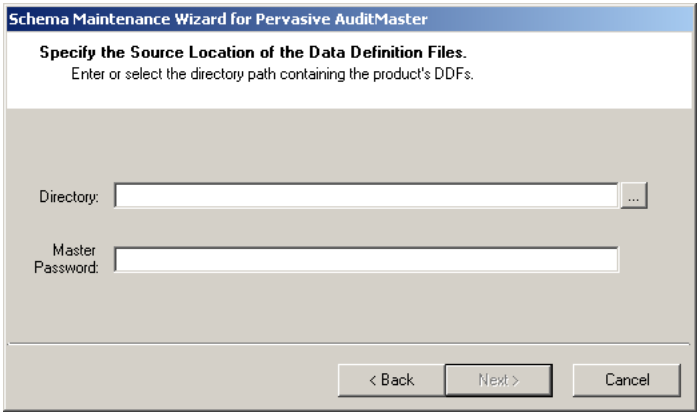
This description will appear in the Product Information area of the Audit Configuration window.

7 Enter a version for the audit configuration.

A version number will help to identify the release of your application and distinguish it from other versions if your network environment supports more than one release.

8 Click **Next**.

The wizard asks for the folder for the schema to be imported.

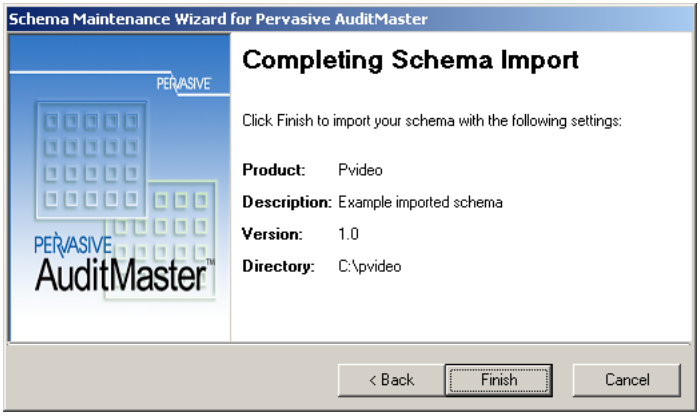

Schema Maintenance Wizard for Pervasive AuditMaster
Specify the Source Location of the Data Definition Files.
Enter or select the directory path containing the product's DDFs.
Directory:
...
Master Password:
< Back
Next >
Cancel

This directory is the location for the database tables and schema information in their data dictionary files (file.ddf, field.ddf, index.ddf).

**9** Enter a directory path name or use the browse button to navigate to the correct folder. If a password is needed to access the database, then enter it here; otherwise, leave it blank.

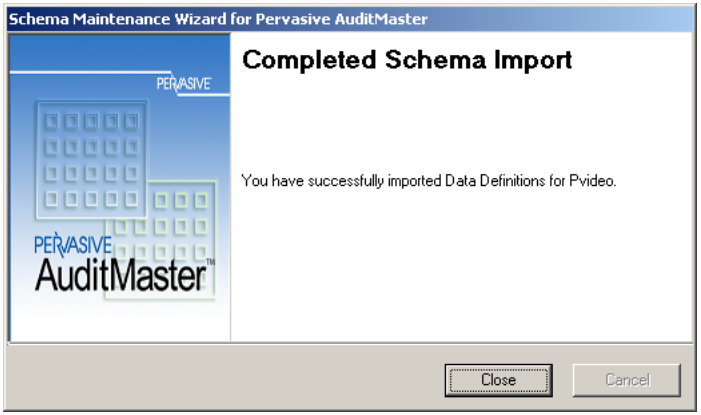
**10** Click Next.

The wizard summarizes the schema import.




**11** Click Finish to complete the import.

The wizard reports the result of the schema import.




**12** Click Close.

When you open the Audit Configuration window, the imported schema will appear and be ready for use.

**Note** Schema import does not affect display of data already captured.

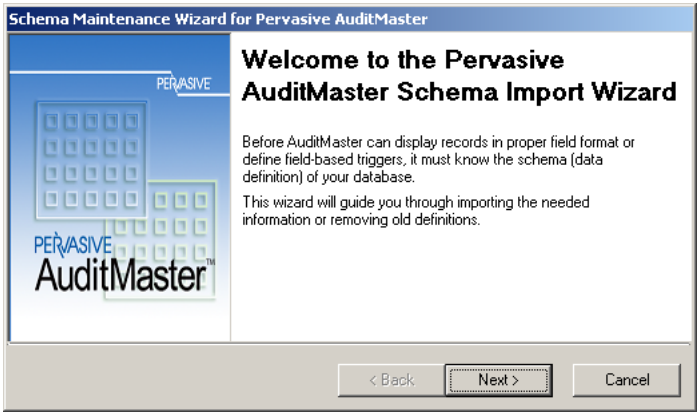
## *Removing a Schema from AuditMaster*

Removing a schema from the AuditMaster system allows you to replace it with a different schema.

### ➢ To remove a schema from AuditMaster

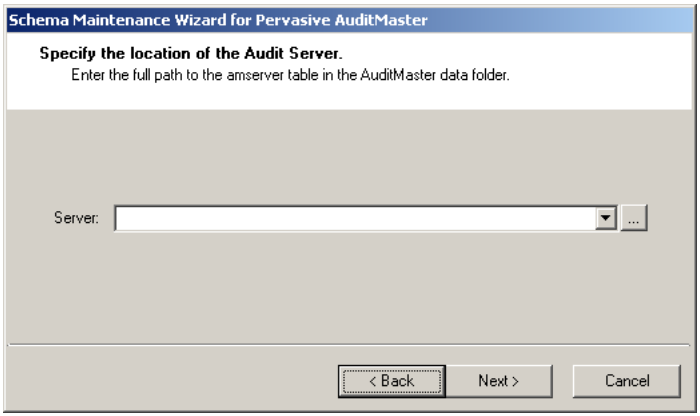
**1** Access Schema Maintenance Wizard from the operating system Start menu or Apps screen..

The Schema Maintenance Wizard appears.


Schema Maintenance Wizard for Pervasive AuditMaster
PERVASIVE
PERVASIVE
AuditMaster™
Welcome to the Pervasive AuditMaster Schema Import Wizard
Before AuditMaster can display records in proper field format or define field-based triggers, it must know the schema (data definition) of your database.
This wizard will guide you through importing the needed information or removing old definitions.
< Back
Next >
Cancel

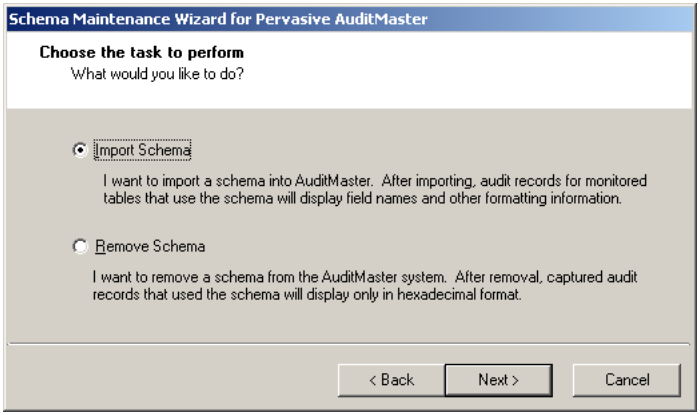
**2** Click Next to continue.

The wizard asks you to specify the location of the amserver file.


Schema Maintenance Wizard for Pervasive AuditMaster
Specify the location of the Audit Server.
Enter the full path to the amserver table in the AuditMaster data folder.
Server:
...
< Back
Next >
Cancel

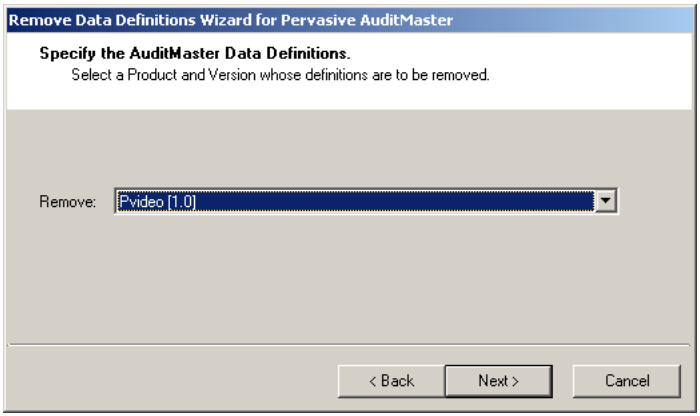
**3** Accept the default path to the file, or enter a custom path, and click Next. You may also use the ellipsis button to browse to a folder or network location.

The wizard asks you to choose to import or remove a schema.


Schema Maintenance Wizard for Pervasive AuditMaster
Choose the task to perform
What would you like to do?
Import Schema
I want to import a schema into AuditMaster. After importing, audit records for monitored tables that use the schema will display field names and other formatting information.
Remove Schema
I want to remove a schema from the AuditMaster system. After removal, captured audit records that used the schema will display only in hexadecimal format.
< Back
Next >
Cancel

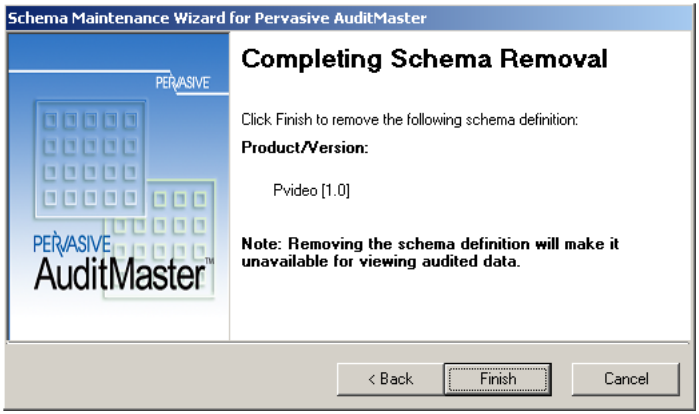
**4** Select Remove Schema and click Next.

The wizard asks for the schema to remove.


Remove Data Definitions Wizard for Pervasive AuditMaster
Specify the AuditMaster Data Definitions.
Select a Product and Version whose definitions are to be removed.
Remove:
Pvideo [1.0]
< Back
Next >
Cancel

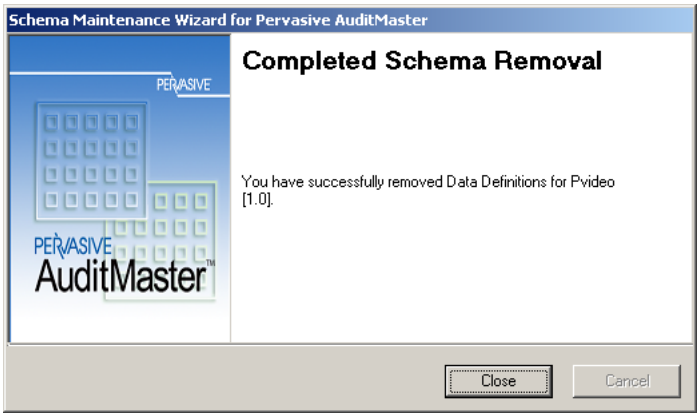
**5** Select the schema from the drop-down list, and click Next.

The wizard summarizes the schema removal.


Schema Maintenance Wizard for Pervasive AuditMaster
Completing Schema Removal
Click Finish to remove the following schema definition:
Product/Version:
Pvideo [1.0]
Note: Removing the schema definition will make it unavailable for viewing audited data.
< Back
Finish
Cancel

**6** Click Finish.

The wizard reports the result of the schema removal.

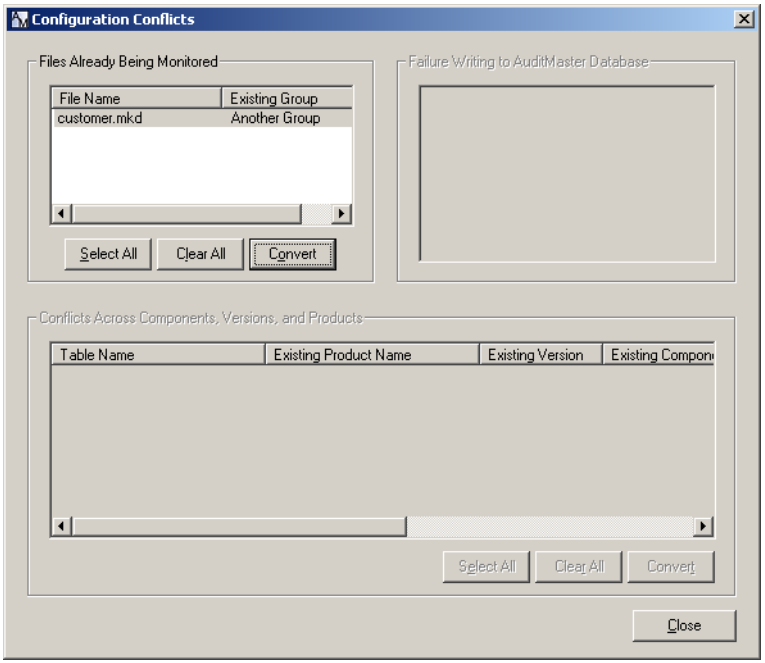

Schema Maintenance Wizard for Pervasive AuditMaster
Completed Schema Removal
You have successfully removed Data Definitions for Pvideo [1.0].
Close
Cancel

**7** Click Close.

**Note** Audit records captured using the removed schema now display as hexadecimal rather than in human-readable format.

# Resolving Configuration Conflicts

Each file selected for monitoring can belong to only one group in one audit configuration. If you attempt to select it for any other group, the following window appears:




You have two options for resolving the conflict:

- Click the Close button to cancel the selection and leave the file in its original group.
- Move the file to the new group by selecting it and clicking the Convert button.

chapter 7

# Querying Audit Records

*How to Work with Audit Records*

This chapter describes tasks that involve running queries against the audit records. Before undertaking these tasks, be familiar with the AuditMaster interface, as described in Chapter 5: Using AuditMaster Viewer.

This chapter covers the following topics:

- Displaying Audit Records
- Working with Archived Audit Records
- Running Queries
- Working with Alerts
- Printing Reports
- Searching Audit Records
- Sorting Audit Records
- Exporting Audit Records to Other Applications
- Displaying Audit Records under Pervasive PSQL Security
- Using AuditMaster Undo

## Displaying Audit Records

AuditMaster monitors application data records for various changes and operations. As it audits these events, it writes audit records to a log file. To access the new records, they are moved to a view file.

Audit records are displayed by queries. A query can include the current view file, one or more archived files, or both current view and archived files. Before querying the current view file, you first should update it to retrieve any new audit records from the log file.

This section covers the following tasks:

- To update the current view file
- To display audit records

### ➢ To update the current view file

**1** In the data tree, right-click the current view file and select Update Current View File, or in the toolbar, select the update current view file icon .

An icon shows that the current view file update is in progress.

**2** Right-click the current view file and select Get File Information.

The tree expands to show information like the following:

You may now query for the audit records you want to display.

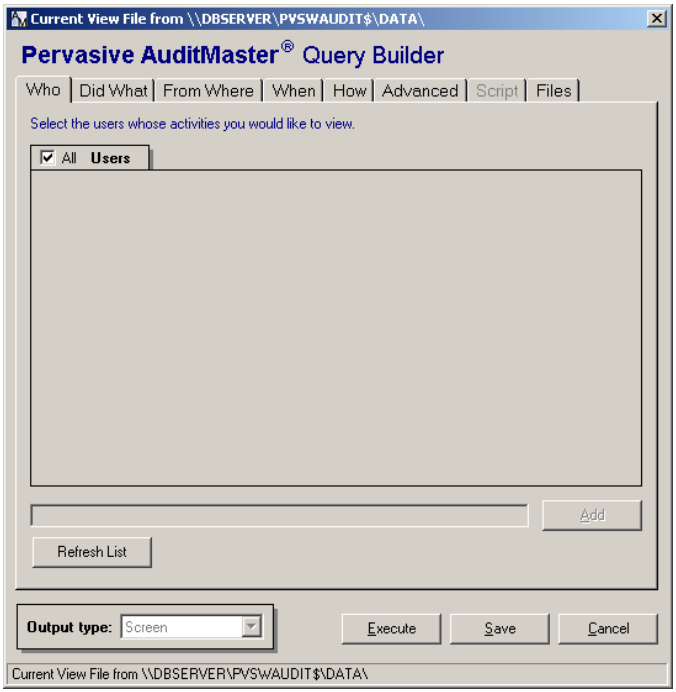
**Note** The Update Status step is optional. However, since the time to finish the update depends on the size of the log file, it may be helpful to verify that the update has finished. For large updates, to be sure that all records are ready for query, update status and then check the status log for the “end of current view file update” message.

### ➢ To display audit records

1. Click the current view file or an archived file in the data tree.
2. Do one of the following:
   - Right-click the file and select Query.
   - Select the File ▸ Query command.
   - In the toolbar, select the new query icon .

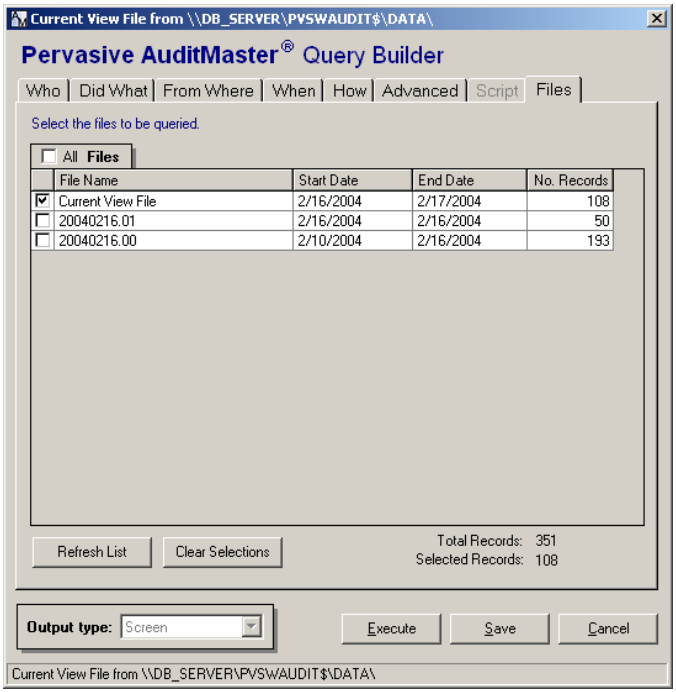
   The Query Builder window appears.

*Figure 7-1 Query Builder*



**3** Click the Files tab to check the range for the query.

The Files tab shows the files available for audit record query.

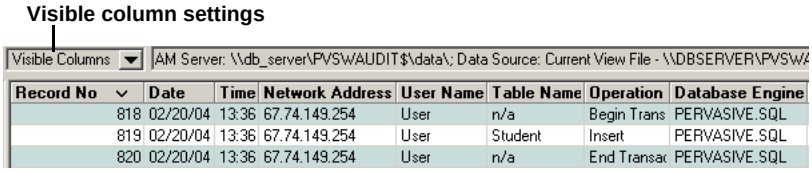



Since the current view file has been chosen, its checkbox is selected. Other examples might include other files.

**4** Click the Execute button at the bottom of the window.

The result of the query appears in the audit record grid.

*Figure 7-2 Sample Audit Record Grid*




To change which record columns are visible, see Working with the Audit Record Grid. To view an individual record in detail, see Viewing Audit Record Details.

## *Working with the Audit Record Grid*

Queries display audit data in the audit record grid. Each column in the grid shows information for each audit record, such as its capture date and time, table name, operation, and user name. The following table provides options for working with and customizing the audit record grid display:

| Option | Steps |
|---|---|
| Setting visible columns in the audit record grid | • Click the Visible Columns drop-down arrow to open or close the list.<br>• Select or clear checkboxes to show or hide particular columns.<br>• Use the ordering buttons to set column order.<br>See Audit Record Columns for more information about individual columns. |
| Changing column order in the audit record grid | Drag and drop each column to the desired position. |
| Searching audit records | See To search audit records |
| Sorting audit records | See To sort audit records |
| Exporting audit records | See To export audit records |

## Audit Record Columns

The following table lists all possible columns for an audit record. The Visible Columns setting determines which ones are displayed in the audit record grid. Column order can be rearranged in Visible Columns, or you can drag and drop columns with the mouse.

*Table 7-1 Visible Column Names in the Audit Data Grid*

| Column Name | Contents |
|---|---|
| Record No. | Incremental number for audit record |
| Dependent Record | Record number for earlier related record:<br>• Modify-before record for modify-after record<br>• Begin-transaction record for end/abort transaction record |
| Date | Capture date for audit record |
| Time | Capture time for audit record |
| Network Address | One of the following:<br>• MAC ID if event in audited file originated on same system as AuditMaster server<br>• IP address for local client applications using UNC address instead of simple path name<br>• IP address if event originated from remote client<br>**Note:** MAC addresses are not available from remote clients in the current release. |
| User Name | Login ID under which event occurred. See Displaying Audit Records under Pervasive PSQL Security. |
| Database Name | Database in which event occurred. See Displaying Audit Records under Pervasive PSQL Security. |
| Table Name | File in which event occurred. The file must be selected for monitoring in an audit configuration. All configured files appear in the Tables list of the Did What tab in Query Builder. |
| Operation | Database event. Events can include any item in the Operations list of the Did What tab in Query Builder.<br>SQL logins display in this column. Selected Pervasive PSQL status codes also appear here when first selected in the Errors to Audit section of the Server Settings window. See details under Maintaining Server Settings. |
| Operation Context | Normal operation or error |
| Database Engine | Either AM Message API (internal use within AuditMaster) or Pervasive PSQL |

*Table 7-1 Visible Column Names in the Audit Data Grid*

| Column Name | Contents |
|---|---|
| Database Version | Version of Pervasive PSQL running on server |
| Product | As listed in audit configuration for monitored file |
| Product Version | As listed in audit configuration for monitored file |
| Group Name | Group for monitored file in audit configuration |
| Component | As listed in audit configuration for monitored file |
| Component Version | As listed in audit configuration for monitored file |
| Process Name | Process that was source of operation |
| OS Version | Name and version of operating system of machine where AuditMaster server is running |
| View File | Location of audit record, either amview (current view file) or archived file name |

## Viewing Audit Record Details

To examine the details of an audit record, click the record in the audit grid to display it in the lower part of the viewer window. If the audit record captures before-and-after changes to an application data record, the detail view shows both versions of the data record, as in the following Demodata example. The Before column shows the original record and the After column shows the change, which is highlighted in red.

Values Before Changes  Values After Changes

| Field Name | Before | After |
|---|---|---|
| ID | 190907350 | 190907350 |
| Cumulative_GPA | 2.000 | 2.000 |
| Tuition_ID | 7 | 7 |
| Transfer_Credits | 0 | 0 |
| Major | Economics | Economics |
| Minor | Computer Science | Computer Science |
| Scholarship_Amount | 0.00 | 1000.00 |
| Cumulative_Hours | 104 | 104 |

## Working with Archived Audit Records

Auditing can generate large numbers of audit records. To manage them, AuditMaster periodically empties the audit log to an archived file. The default archive file size is 75 MB. To reset the default size or choose archiving by date, see Automated Archiving.

Archived files for each server appear in the data tree. The file name uses creation time in the format *yyyymmdd.nn*, where *yyyy* is the year, *mm* is the month, *dd* is the day, and *nn* is the number of the archive file created that day, starting with zero.

Compressing archived files saves as much as 90 percent disk space. AuditMaster encrypts compressed archived files to restrict access to users within the AuditMaster system. Moving an archived file out of its folder (i.e., \Arch or \Comp in the installation directory) grays out its entry in the data tree. Moving it back restores the entry and enables queries again. Permanently deleted files cannot be restored.

The data tree provides several archived file commands. As shown in the following table, right-clicking an archived file offers commands depending on whether the file is compressed. Queries may be run only on uncompressed files.

*Table 7-2 Right-Click Commands for Archived Files in the Data Tree*

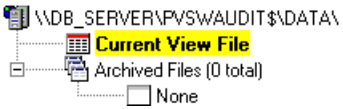
| Command | Uncompressed | Compressed |
|---|---|---|
| **Query**. Run a query against the file. | Yes | No |
| **Execute Saved Query**. Run a saved query. | Yes | No |
| **Compress**. Compress the file. | Yes | No |
| **Decompress**. Decompress the file. | No | Yes |
| **Delete**. Remove the file permanently. | Yes | Yes |
| **Get File Information**. Expand the data tree to show compression status, number of records, file size, last record in archive, and date range of included records. | Yes | Yes |

AuditMaster provides two ways to create archived files:

- Using the Data Tree to Archive Audit Records
- Using Archive Manager

## *Using the Data Tree to Archive Audit Records*

When you first install an AuditMaster event handler and its server appears in the data tree, no audit records have been archived. If you expand Archived Files, the number of archived files is zero.




After you begin logging, audit records may be archived. The system automatically creates an archived file when the audit log reaches a set limit by size or by date and time. You can also archive manually.

**Note** In the data tree, you may sometimes need to right-click the Archived Files icon and select Refresh All to update the list.

This section covers the following tasks:

- To archive manually
- To set the number of archived files to show

To automate archiving, see Automated Archiving.

### ➢ To archive manually

You may want to archive manually for the following reasons:

- The audit log has grown large, queries and other operations take longer, and you don't want to wait until the next automated archiving to regain performance speed.
- Automated archiving will not occur soon, but an event of interest makes it preferable to archive now.
- You wish to archive and compress records to manage disk space.

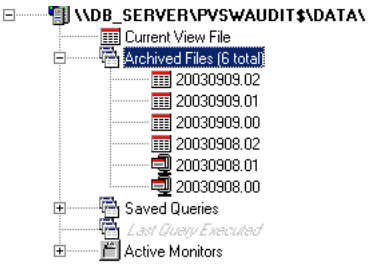
In the data tree, select the current view file and do one of two things:

- Select Server ▸ Archive Current View File, or right-click the file and select Archive.
- Select Server ▸ Archive & Compress Current View File, or right-click the file and select Archive & Compress. Large numbers of records can take time, so you may want to use Admin ▸ View Status Log command to check for the "finished compressing" message.

You cannot run a query against a compressed archive file. You must first decompress it by right-clicking and selecting Decompress.

### ➤ To set the number of archived files to show

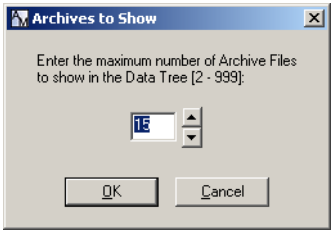
You can control the number of archived files listed in the data tree, which displays both uncompressed and compressed archived files.




The default setting for the number of archived files displayed in the list is 15. Displaying a shorter list does not delete archived files but only removes them from the display. They remain in the \Arch and \Comp folders in the AuditMaster root directory (e.g., default C:\<*installation directory*>\Audit). Raising the number in the setting displays them again.

**1** Select View ▸ Set Archives to Show.

The Archives to Show dialog box appears.



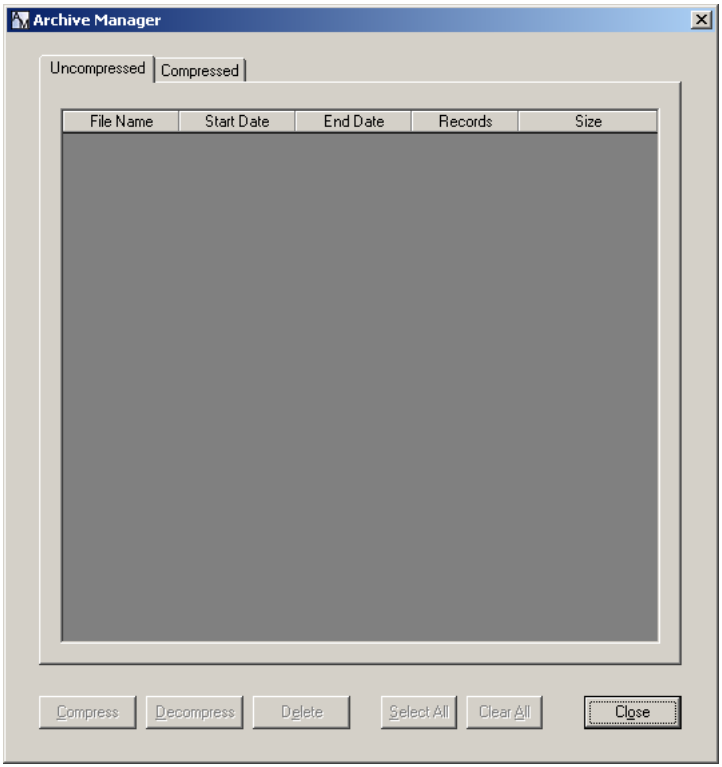

**2** Set the maximum number of archives to show, and click OK.

**Note** In the data tree, you may need to right-click the Archived Files icon and select Refresh All to update the display.

## *Using Archive Manager*

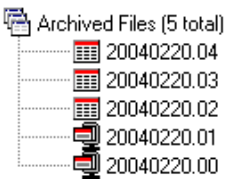
Archive Manager is a tool for handling audit archives. Before using it, first read Working with Archived Audit Records.

In the data tree, you handle one archived file at a time, but Archive Manager allows you to work with several archived files as a group. The Tools ▸ Archive Manager command displays its window.

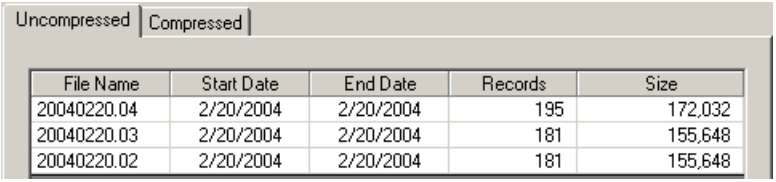



This example corresponds to Archived Files in the data tree:

After auditing has occurred, the data tree might appear like this:

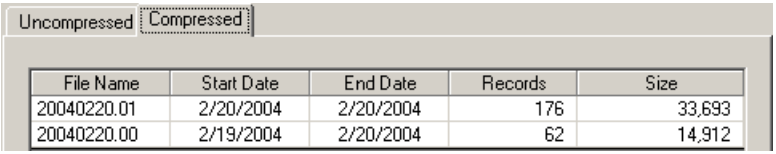


And the Uncompressed tab would show this:




| File Name | Start Date | End Date | Records | Size |
|---|---|---|---|---|
| 20040220.04 | 2/20/2004 | 2/20/2004 | 195 | 172,032 |
| 20040220.03 | 2/20/2004 | 2/20/2004 | 181 | 155,648 |
| 20040220.02 | 2/20/2004 | 2/20/2004 | 181 | 155,648 |

While the Compressed tab would show this:




| File Name | Start Date | End Date | Records | Size |
|---|---|---|---|---|
| 20040220.01 | 2/20/2004 | 2/20/2004 | 176 | 33,693 |
| 20040220.00 | 2/19/2004 | 2/20/2004 | 62 | 14,912 |

In each case, the appropriate buttons are available at the bottom of the Archive Manager window:

| **Command** |
|---|
| **Compress**. Compress the file. |
| **Decompress**. Decompress the file. |
| **Delete**. Remove the file permanently. |
| **Select All**. Highlight all files in the list. |
| **Clear All**. Clear highlighting on selected files. |
| **Close**. Close Archive Manager. |

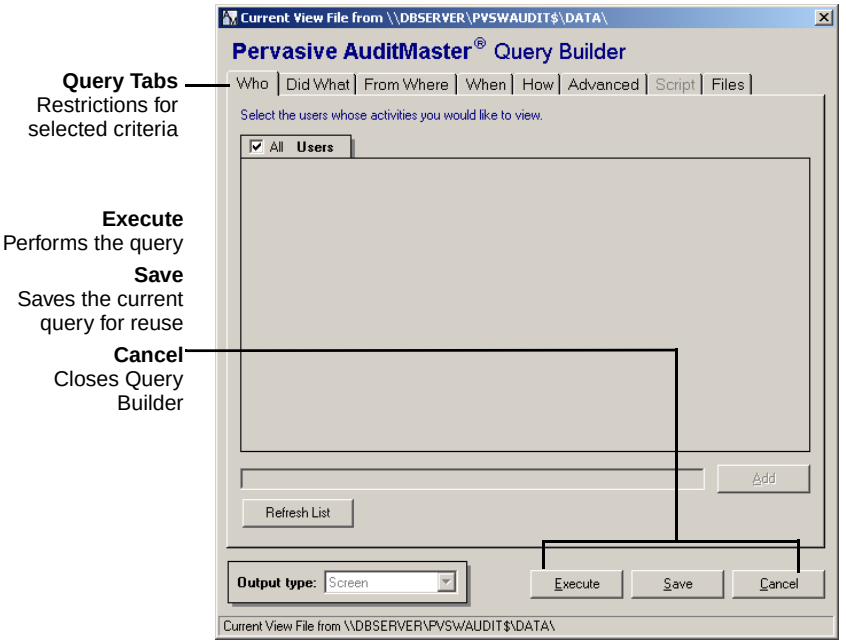
To use Archive Manager, click a button command after clicking a file to highlight it. Use the SHIFT key to select a range of files or the CTRL key to add a single file to the currently highlighted selection.

**Note** The larger the file, the longer it takes to decompress and become ready to query. For large files, to be sure all records are ready, select Admin ▸ View Status Log to check the log for the "finished decompressing" message, even if the file icon shows as uncompressed. You may also want to right-click Archived Files in the data tree and select Refresh All to update the display.

# Running Queries

To display audit records from a current view or archived file, you must first run a query using AuditMaster Query Builder. You may query for all available audit records in the files you select, or you may restrict the query to Who, Did What, From Where, When, or How. For example, you can search for audited events on a particular date, events from a selected table, or changes that were made by only one particular user.

*Figure 7-3 Query Builder Window*




This section covers the following topics:

- Displaying All Audit Records
- Restricting a Query
- Building an Advanced Query
- Using the Files Tab
- Running a Saved Query or Last Query Executed

## Displaying All Audit Records

The simplest query in the Query Builder window is to display all audit records:

### ➤ To display all available audit records

1. Select a current or archived view file.
2. Select File ▸ Query, or right-click and select Query.

   The Query Builder window appears.
3. By default, all options in each tab are selected. To display all AuditMaster data for this file, simply select Execute.

   Audit records are displayed in the grid in the upper right-hand pane of the viewer.

## Restricting a Query

Query Builder provides tabs for restricting a query to who, did what, from where, when, how, and in which audit record files to look.

### ➤ To restrict a query

1. Select options from the tabs to make a query more selective.

*Table 7-3 Options for Restricting a Query*

| To find... | Click tab | Perform these steps... |
|---|---|---|
| **Users**<br>All records that contain a specific user or users | **Who** | 1. To find a specific user or users, clear the **All Users** option.<br>2. The list of database users is now available.<br>3. Select a user or multiple users by checking the box beside their name.<br>4. If needed, you can add a user by clicking **Add** and typing in the specific user. |

*Table 7-3 Options for Restricting a Query*

| To find... | Click tab | Perform these steps... |
|---|---|---|
| **Operations, Groups, and Tables**<br>Specific operations, such as an insert or a delete, in a specific type of table, in a specific group | **Did What** | 1. To find a specific type of operation, clear the **All Operations** option. You can also clear the **All Groups** or **All Tables** option. The list is now available.<br>2. Select the operations and any objects affected by them. Expand lists as needed to select the appropriate options. Use the SHIFT or CTRL keys to extend the selection. |
| **Network Addresses**<br>Any information originating from a specific network address. | **From Where** | 1. To find a specific network address, clear the **All Network Addresses** option. The list of network addresses is now available.<br>2. Select one or more network addresses by checking the box beside the address. If needed, you can add an address by clicking **Add** and typing in the specific network address. |
| **Specific Dates**<br>Any activity on a specific date and within a time range | **When** | 1. To find a specific start and end date, clear the All Date Range option. The Start Date and End Date calendars are now available.<br>2. Select a day, month, and year from the calendars. Use the arrows to click back and forth through the months.‘<br>3. To find a specific time range for each day in the date range, clear the Time Range option. Select a time from the Start Time and End Time fields.<br>**Note:** The time range applies to each individual day in the date range (e.g., 8:00 a.m. to 5:00 p.m. on each day). |
| **Processes or Programs**<br>The program or process identified by AuditMaster in the Process Name column of the audit record grid | **How** | 1. To find a specific program or process, clear the **All Processes** option. The processes are now available.<br>2. Select a program or process by clicking the box beside the option. If the process name does not appear, use the **Add** field at the bottom of the pane to include it in the list. |

2 If you plan to reuse this query later, click Save.

In the save dialog box, provide a descriptive name for the query and click OK. For details on using a saved query, see Running a Saved Query or Last Query Executed.

3 To run the query, click Execute.

The audit record grid displays the query result.

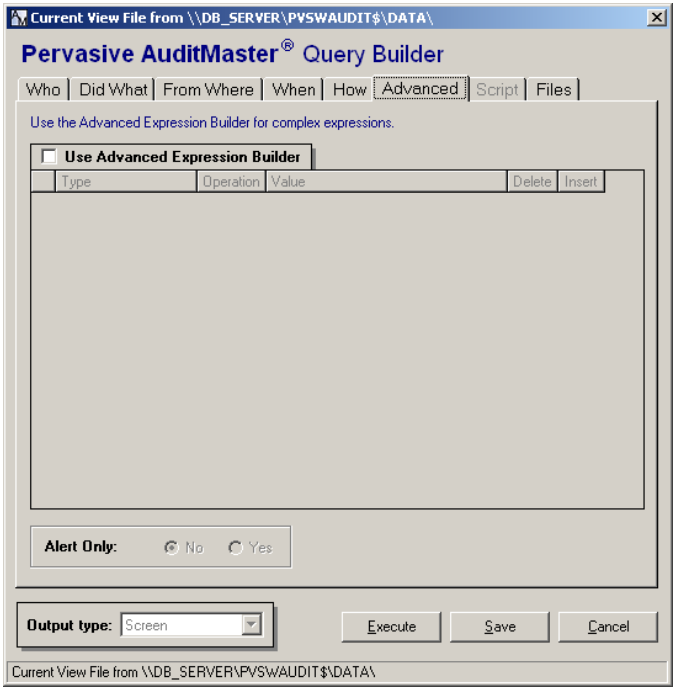
## Building an Advanced Query

The Advanced tab is used to build complex queries that cannot be built using the other tabs. This tab can set expressions to evaluate for specific events and can also be used to query at the column level in an audited table if its schema has been imported.

The following example shows the creation of a query to search for all inserts into the database on a specific day.

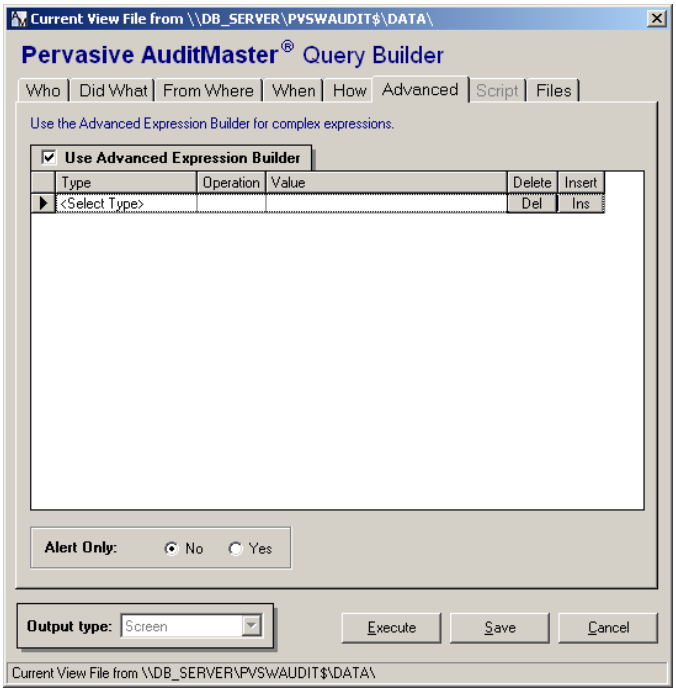
### ➤ To step through the Advanced Expression Builder example

1 Open the Query Builder window, and click the Advanced tab.



**2** To customize your query, select the Use Advanced Expression Builder checkbox.

The expression area becomes active.




**3** In the Type column, double-click Select Type to activate a drop-down list for the following query attributes:

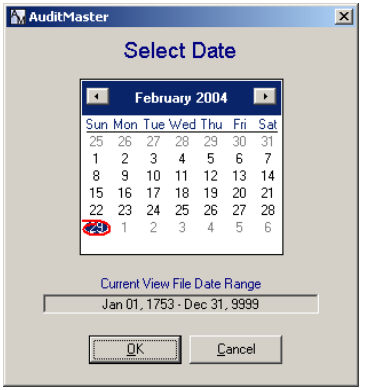
| Select Type Attribute | Description |
|---|---|
| ( | Open parenthesis to build expression block |
| Data Field | Same as field attribute from Tables under Did What tab, except that you can restrict the query at the column level, not just at the table level |
| Date | Same as Date Range attribute under When tab |
| Group | Same as Groups attribute under Did What tab |
| Database Name | Pervasive PSQL database where event occurred |
| Table | Same as Table attribute under Did What tab |
| Operation | Same as Operations attribute under Did What tab |

| Select Type Attribute | Description |
|---|---|
| How | Same as Process attribute under How tab |
| Rec ID | Record number in audit data grid |
| Time | Same as Time Range attribute under When tab |
| Where | Same as Network Address attribute under From Where tab |
| Who | Same as User attribute under Who tab |
| and | Used to build expression |
| or | Used to build expression |
| ) | Close parenthesis to build expression block |

**Note** All text values entered for Select Type are case-sensitive. For example, using defaultdb as the database name returns no result, since it does not match case with the name DefaultDB.

**4** In the list of query attributes, select Date.

A calendar dialog box appears with the current date selected.

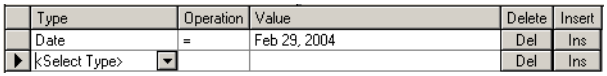

AuditMaster
Select Date
February 2004
Sun Mon Tue Wed Thu Fri Sat
25 26 27 28 29 30 31
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 1 2 3 4 5 6
Current View File Date Range
Jan 01, 1753 - Dec 31, 9999
OK
Cancel

**5** Click OK to accept the default date.

The date appears in the Value column.

6 In the Operation column, select a logical operator, or leave the default equal sign = as is.

The expression should resemble the following:




7 You may use the Del and Ins buttons to remove an item from the expression or add a new item.

8 After building your expression, decide whether to set it for Alert Only.

This option will select for records meeting the defined conditions but display only those for which alerts have tripped.

For more details, see Working with Alerts.

9 If you plan to run this query often, click Save.

The Saved Queries window appears to enable you to give the query a name and save it for future use. See also Running a Saved Query or Last Query Executed.

10 To run this query, click Execute.

The Query Builder executes the query and displays the results in the audit record grid.

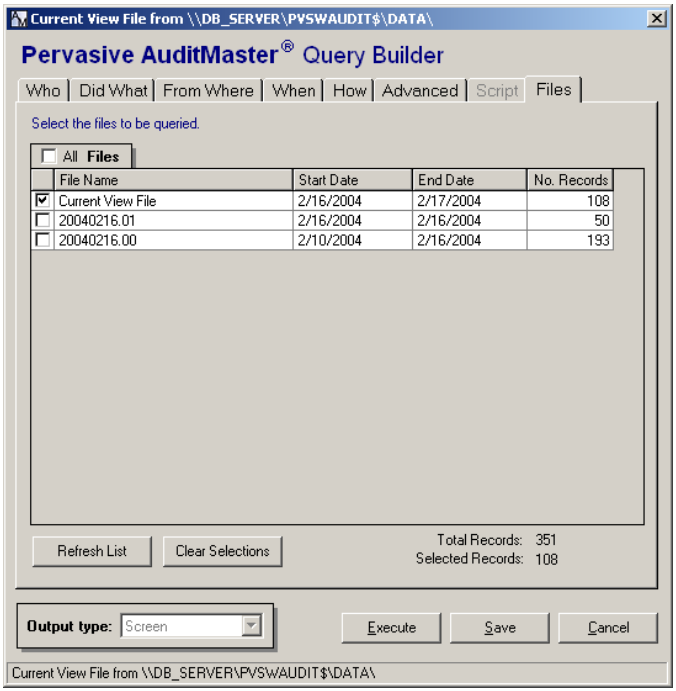
## Using the Files Tab

The Files tab allows you to select which current view and uncompressed archived files to include in a query.

### ➤ To select which files to include in a query

1 From the Query Builder window, click the Files tab.

*Figure 7-4 Files Tab*




2 Click checkboxes to make or clear file selections for the query, then continue with query settings in other tabs as needed.

Only uncompressed files can be queried. If a file you want to query is not listed, you will need to decompress it.

**Note** The larger the file, the longer it takes to decompress and become ready to query. For large files, to be sure that all records are ready, use the Admin ▸ View Status Log command to check the status log for the "finished decompressing" message, even if the file icon shows as uncompressed. You may also want to right-click the Archived Files branch of the data tree and select Refresh All to update the display.

## *Running a Saved Query or Last Query Executed*

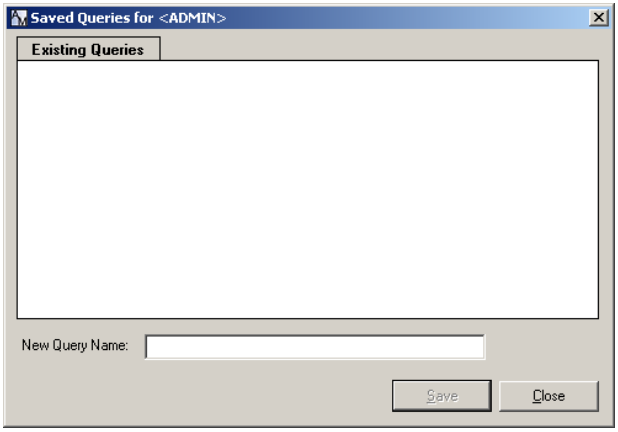
For each AuditMaster server, queries are stored in the data tree under Saved Queries and Last Query Executed. This section covers the following topics:

- To save a query
- To use a saved query
- To use the last query executed

### ➢ To save a query

1 After creating a query in the Query Builder window, click the Save button.

The Saved Queries dialog box asks you to name the query.




2 Enter a name for the query and click Save.

The query is added to the list of existing queries and will now appear in the data tree.

**3** Click Close.

### ➤ To use a saved query

**1** In the data tree, right-click a query under Saved Queries.

A pop-up menu offers you several choices.

**2** Select one of the options listed in the following table:

*Table 7-4 Saved Query Commands*

| Command |
|---|
| **Query Current View File**. Run the query against the current view file. |
| **Query Multiple View Files**. Display the Files tab in the Query Builder to select the files against which to run the query. |
| **Rename**. Change the name of the query. |
| **Delete**. Remove the query permanently from the list. |

If you run a query, any result appears in the audit record grid. You may simply double-click a saved query to run it against the current view file.

Only uncompressed files can be queried. If a file used in a query has been compressed, you must decompress to run the query.

**Note** The larger the file, the longer it takes to decompress and become ready to query. For large files, to be sure that all records are ready, use the Admin ▸ View Status Log command to check the status log for the "finished decompressing" message, even if the file icon shows as uncompressed. You may also want to right-click the Archived Files branch of the data tree and select Refresh All to update the display.

### ➤ To use the last query executed

In the data tree, double-click the Last Query Executed.

Any result appears in the audit record grid.

# Working with Alerts

Under Microsoft Windows, AuditMaster provides an alert capability. The Alerts window enables you to create an alert to a specific event in a Pervasive PSQL database. Once an alert is set, AuditMaster checks each new audit record for the alert condition. When found, AuditMaster executes an alert action. For example, when a data record is deleted, the system can send an alert to notify you by email. In the audit record grid, tripped alerts are flagged with an icon .

**Caution** Dramatic and undesirable consequences may arise from an alert with a broad query likely to match a large number of audit records, especially when the alert action sends email.

This section covers the following topics:

- Adding a New Alert
- Setting an Action for an Alert, including
  - Setting an EmailAlert Action
  - Setting a RunProgram Action
- Editing an Existing Alert
- Stopping an Alert

**Note** After creating or changing an alert, close AuditMaster Viewer and restart the AuditMaster event handler so that the alert takes effect. See Restarting the AuditMaster Event Handler.

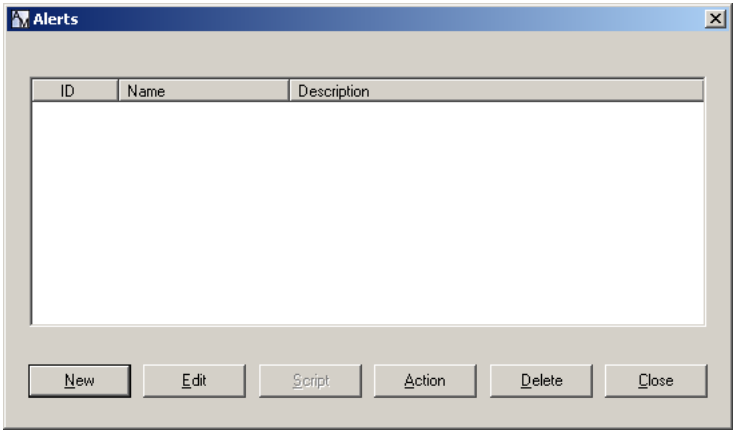
## Adding a New Alert

### ➢ To create an alert

1 In AuditMaster Viewer, run a query to display the type of audit records for which you would like to create an alert condition.

2 Select File ▸ Alerts.

The Alerts window appears.




3 Click New.

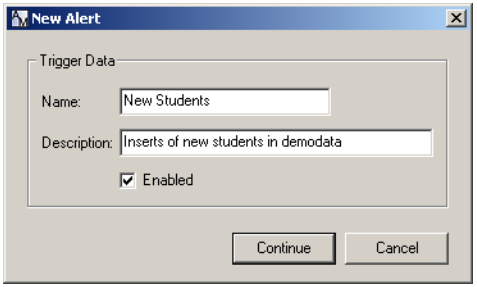
The New Alert window appears.

4 Enter a name for this alert using letters, numbers, or spaces.

In this example, we create an alert for new students in the Pervasive PSQL demonstration database.

5 Enter a description for the alert using letters, numbers, or spaces.

We suggest you describe the event for which the alert is to watch.

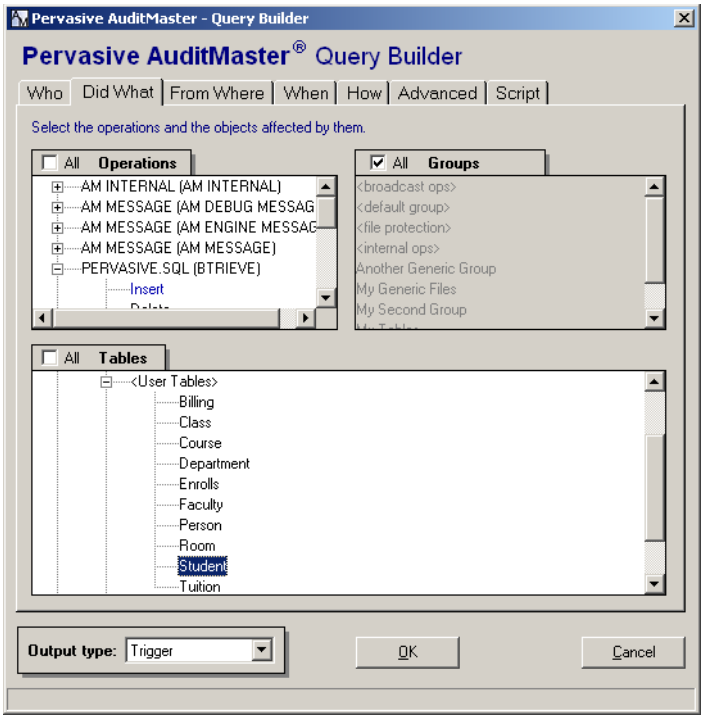


**6** Click Continue.

The Query Builder window appears.

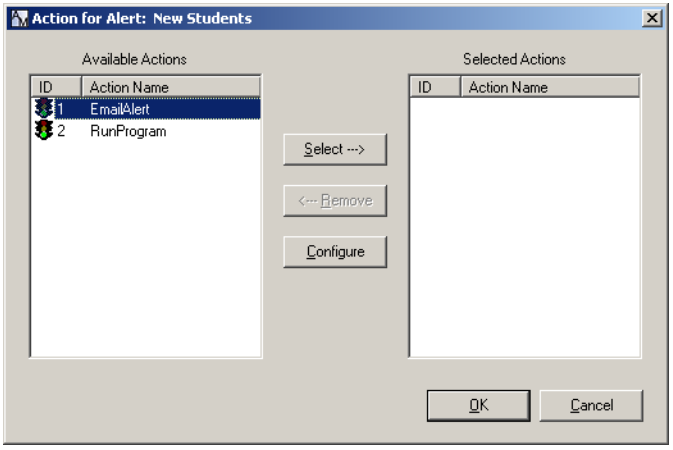
**7** Define the criteria for this alert using the tabs in the Query Builder.

For details on using these tabs, see Running Queries.



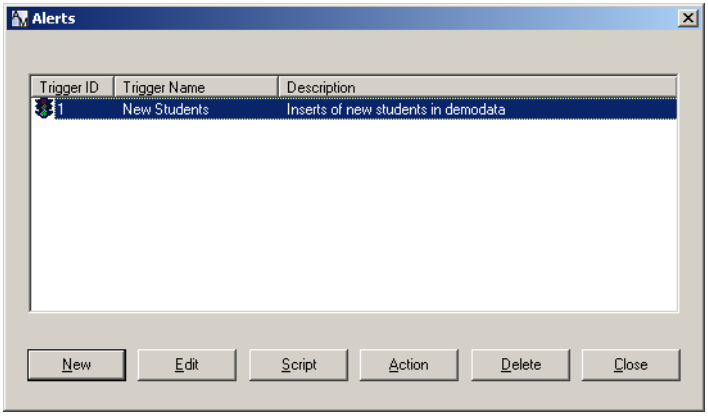
**8** When you are finished, click OK.

The Action for Alert window appears.




**9** At this point, you may select and configure an alert action to set for this alert, but for now simply click OK and continue with the tutorial steps.

The Alerts window shows the alert that was just added.




**10** You can now choose from one of the following tasks:

- Setting an Action for an Alert.
- Editing an Existing Alert.
- Stopping an Alert.

## *Setting an Action for an Alert*

Once you have added an alert, you need to set an action to be performed each time AuditMaster finds a match for the alert condition.

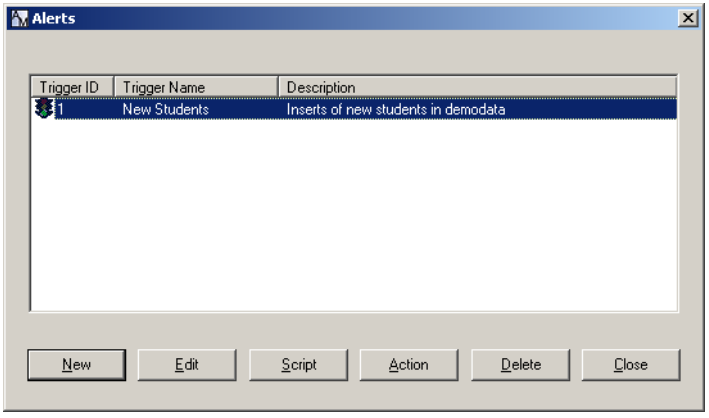
You can set one or both of two actions for each alert:

- Setting an EmailAlert Action
- Setting a RunProgram Action

**Note** From a viewer client on the server machine where AuditMaster is running, you can set actions both to send email or run a program on the server; however, from a remote viewer client you are unable to set an action to run a program on the server and can set only email alerts.

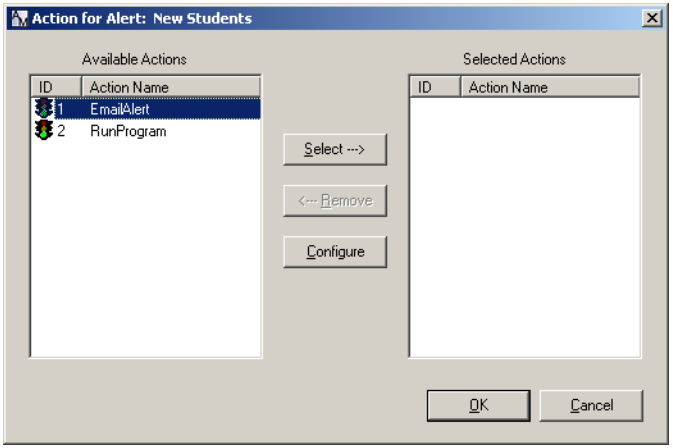
### ➤ To set an action for an alert

1 Select File ▸ Alerts if the Alerts window is not open, and select an alert to configure.



**2** Click Edit.

The Action for Alert window appears.




**3** Select at least one of the built-in alerts, and click the Select button:

- EmailAlert
  The EmailAlert action sends an email to a specified group of addresses when an alert condition is met. To configure the email alert action, proceed to Setting an EmailAlert Action.
- RunProgram
  The RunProgram action runs a specified program on the server when an alert condition is met. To configure the program, proceed to Setting a RunProgram Action.

**4** Click OK.

Selected actions are now set for the alert and will be performed if the alert condition is met.

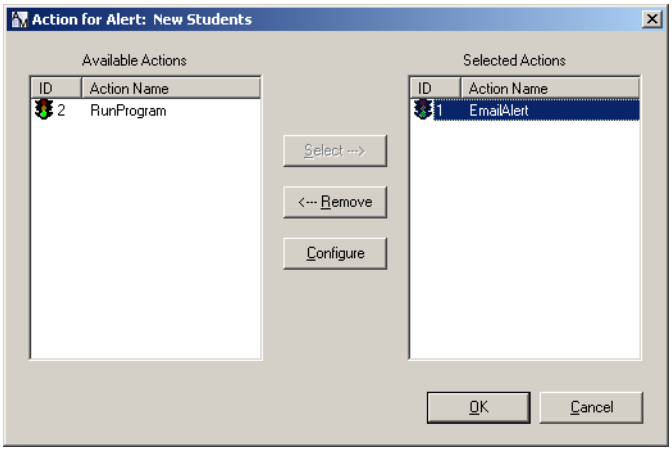
**Note** After creating or changing an alert, close AuditMaster Viewer and restart the AuditMaster event handler so that the alert takes effect. See Restarting the AuditMaster Event Handler.

## Setting an EmailAlert Action

### ➤ To set email groups and addresses for an alert

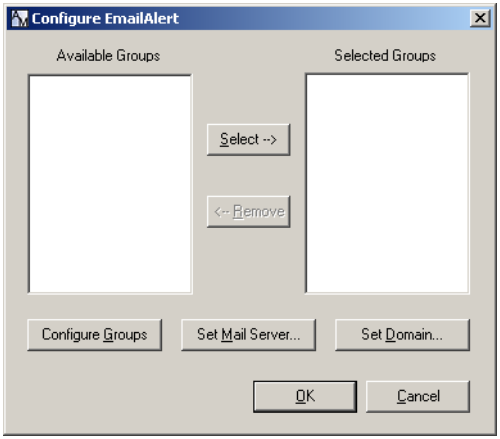
**1** If the Alerts window is not open, select File ▸ Alerts, select the alert to configure, click the Action button, click EmailAlert, and click the Select button.

The EmailAlert action moves to the Selected Actions column.




**2** With the EmailAlert item selected, click the Configure button.

The Configure EmailAlert window appears.



3 If an email group to which you want to send alerts exists in the list, simply select it, click the right arrow (>) to move it to Selected Groups. You may also double-click the group name.

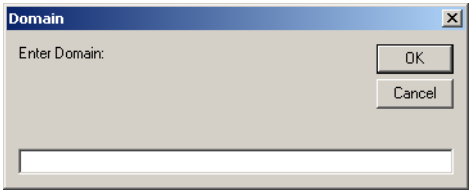
When the alert condition is met, addresses in this group will receive email.

4 To set the SMTP server used to send out-going mail, click Set Global SMTP Server.

5 Add the server name for the SMTP server, and click OK.

For example, if your out-going mail server is named smtp-server.companyname.com, then enter `smtp-server` in this field.

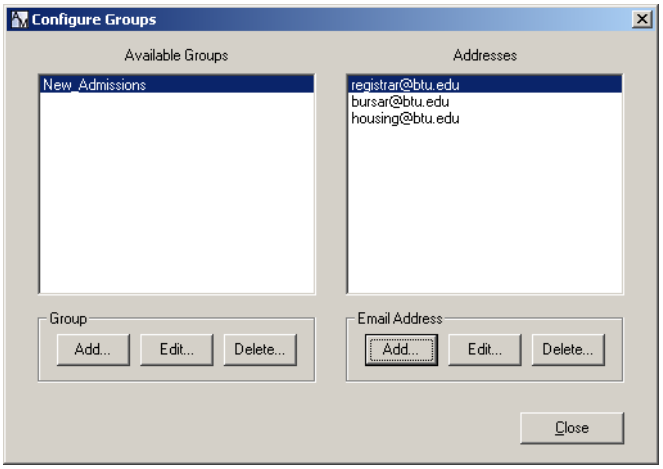
6 To set the global domain used by your company, click Set Global Domain.




7 Add the domain name, such as pervasive.com, and click OK. Continuing with the example from the last step, here you would enter `companyname.com`.

**8** To configure a group, click Configure Groups.

The Configure Groups window appears. For this demonstration, sample values have been filled in.

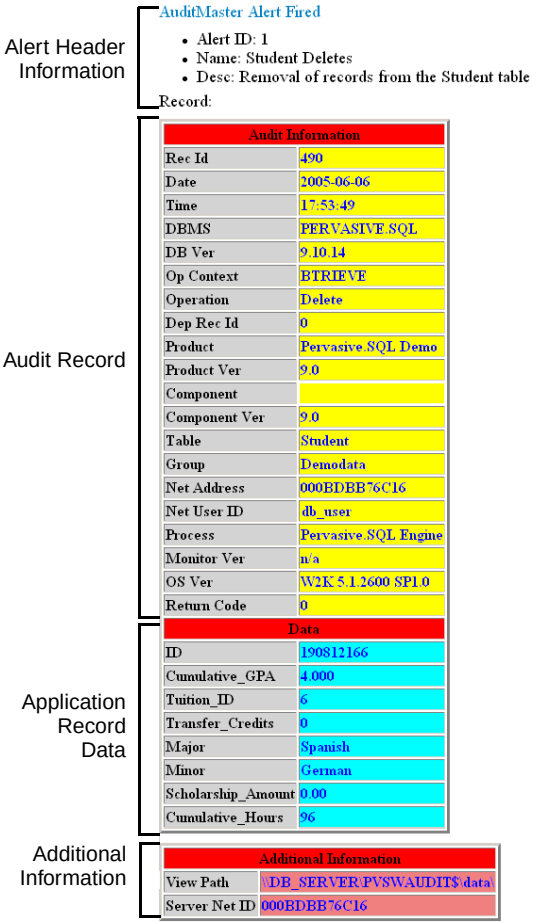



**9** In this window you can manage email groups and addresses, as described in the following table. When you are finished, click OK to return to the Configure EmailAlert window.

| Email Task | Steps |
|---|---|
| **Add New Group** | Click **Add New Group**, enter a name for the new group, and click **OK**. |
| **Edit Group Name** | Select a group name, click **Edit Group Name**, enter a new name for this group, and click **OK**. |
| **Delete Group** | Select a group name, click **Delete Group**, and click **Yes** to confirm. The group is deleted only for this alert and remains in the system for use in other alerts. |
| **Add New E-mail Address** | With a group selected, click **Add New E-mail Address**, enter the email address, and click **OK**. |
| **Edit E-mail** | With a group selected, select an address from the list of email addresses for that group, then click **Edit E-mail**, enter a new email address, and click **OK**. |
| **Remove E-mail Address** | With a group selected, select an email address, click **Remove E-mail Address**, and click **Yes** to confirm. |

The following sample email alert was tripped by an insert in the Demodata database. If AuditMaster monitors a database without a schema, the application record data in the alert does not display the hexadecimal content. If the schema has been imported, then column names are displayed.

*Figure 7-5 Structure of an Email Alert*

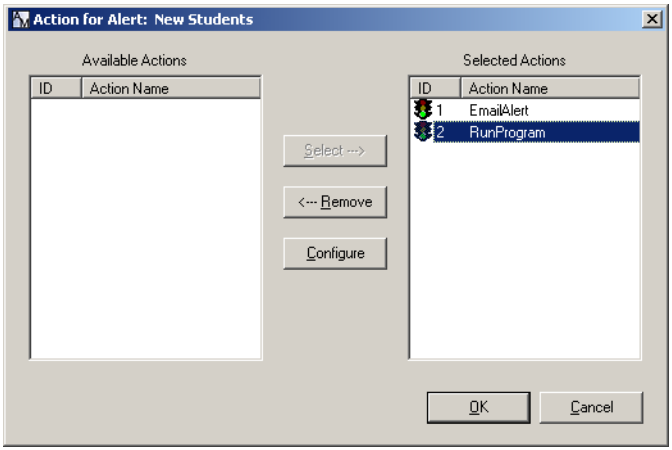


## Setting a RunProgram Action

### ➤ To set a program to run as an alert action

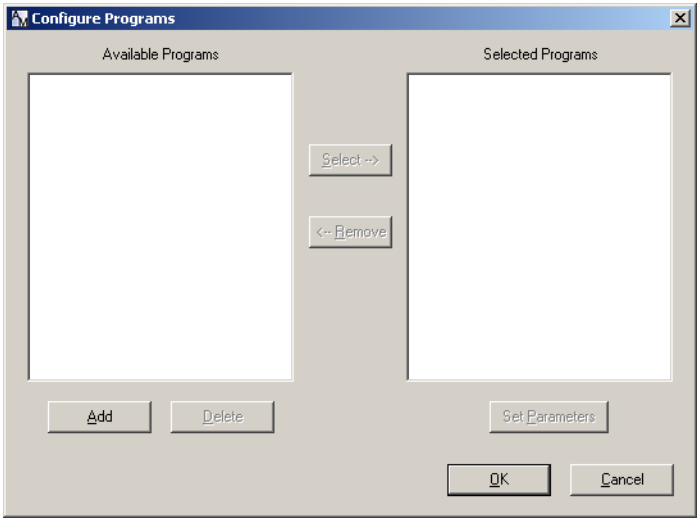
**1** If the Alerts window is not open, select File ▸ Alerts, select the alert to configure, click the Action button, click RunProgram, and click the Select button.

The RunProgram action moves to the Selected Actions column.




**2** With the RunProgram item selected, click the Configure button.

The Configure Programs window appears.



**3** In the Configure Programs window you can select programs to run on the Pervasive PSQL server as alerts as described in the following table.

| To... | Steps |
|---|---|
| **Select a program to run** | 1. Click one of the available programs, and click the **Select** button.<br>2. The program is moved to the Selected Programs list. When the condition for this alert is met, this program will be executed on the server. |
| **Add a new program to the list of Available Programs** | 1. Click the **Add** button.<br>2. The Select an Executable File window appears, pointing to the C: directory on the server.<br>3. Select a program, or browse and find another.<br>4. When you have selected the program, click **OK**. |
| **Remove a program from the list of Available Programs** | 1. Select the program name.<br>2. Click **Remove**.<br>3. Click **Yes** to confirm. |
| **Set parameters for a program in the Selected Programs list**<br>Use this option only if you are very familiar with program parameters. | 1. Select the program name.<br>2. Click **Set Parameters**.<br>3. Click the buttons to **Add**, **Remove**, or **Change** parameters for the program to be run.<br>4. Enter any new or changed parameter in the field provided, and click **OK**. |

**4** When you are finished selecting and configuring a program to run as an alert, click OK to return to the Action for Alert window.

**5** Click Close to exit from the Alerts window.

## *Editing an Existing Alert*

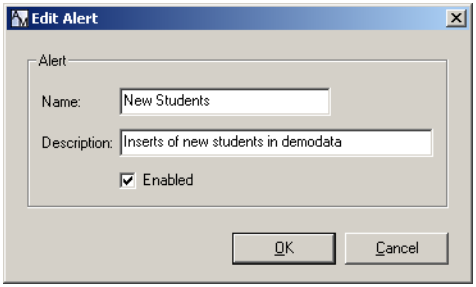
You can edit the name and description of an alert. However, you cannot change the conditions for the alert. To monitor for a different event, delete the old alert and enter a new one.

### ➤ To change an alert name or description

1 In the Alerts window, select an alert from the list, and click the Edit button.

The Edit Alert window appears.

*Figure 7-6 Edit Alert Window*




2 Edit the name and description for this alert, and click OK.

## Stopping an Alert

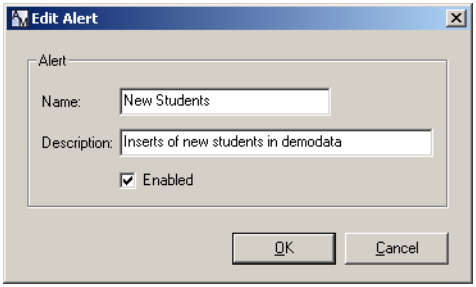
To stop an alert from running, you can disable its action or delete the alert entirely.

**Note** Deleting an alert does not delete any email group associated with its action. Email groups associated with an EmailAlert action remain in the system for use with other alerts.

### ➤ To disable an alert action

1 Select a alert from the Alerts window, and click the Edit button.

The Edit Alert window appears.




2 Clear the Enabled checkbox, and click OK.

The alert action is disabled. You can enable it again later.

### ➤ To delete an alert

1 Select an alert from the Alerts window list.

Click the alert to select it.

2 Click the Delete button.

A window prompts you to confirm the deletion.

3 Click Yes to confirm.

The alert is deleted and can no longer run.

# Printing Reports

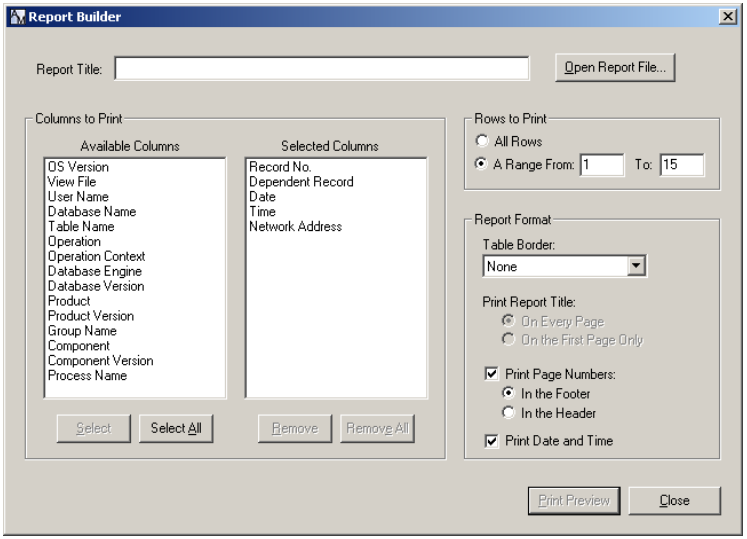
AuditMaster lets you print reports from the audit record grid.

1 Run a query and then select a range of columns and rows displayed in the audit record grid.

2 Select File ▸ Report.

The Report Builder window appears.

*Figure 7-7 Report Builder after Running a Query and Selecting Audit Records*




3 If you want to load and customize a saved report, click the Open Report File button and select the settings file for an existing report.

The report is loaded.

4 In the Report Title field, enter a name for this report.

This name will appear at the top of your printout.

5 From the Available Columns list, select the columns to include in this report.

You may select up to 30 columns. If you already selected a range of columns and rows, these are listed under Selected Columns. You may double-click other column names to move them to Selected Columns. Clicking Select All moves over all columns.

6 Select the Rows to Print.

- All Rows. Click to select all rows of the columns you selected.
- A Range of Rows. Click to define a range of rows and change the row numbers shown, which by default indicate the rows you highlighted in the audit record grid before you opened Report Builder.

7 Under Report Format, set the appearance of the report.

- Table Border. If you want the tables to have borders, select the border type from the drop-down list.
- Print Page Numbers. Check the box beside the option to include the page number. Select whether to print the page number in the Left Footer or Left Header of the printout, as well as whether to include Date and Time.
- Print Report Title. Select whether you want the report title to appear On Every Page or On the First Page Only.
- Print Date and Time. Select if you want the date and time to appear in the footer of each printed report page.

8 When you are finished, click Print Preview.

The Report Print Preview window displays the report on-screen as it will be printed.

9 From the File menu in the Report Print Preview window, you may do the following:

- Select Save Report As to save the current report settings for future reuse.
- Select Open Report to use the settings in a saved report.
- Select Page Setup to adjust standard page settings.
- Select Print Setup to adjust standard printer settings.
- Select Print to print the report.
- Select Exit to return to Report Builder.

# Searching Audit Records

You can use the search command to find particular users, operation types, or values for the current audit records grid view. AuditMaster uses a sophisticated search engine, so it is easy to use different search options and directions. Searches can also be made case-sensitive.

**Note** Depending on the number of records and the complexity of the search criteria, it may take some time to complete your search. Whenever possible, try to narrow your criteria.

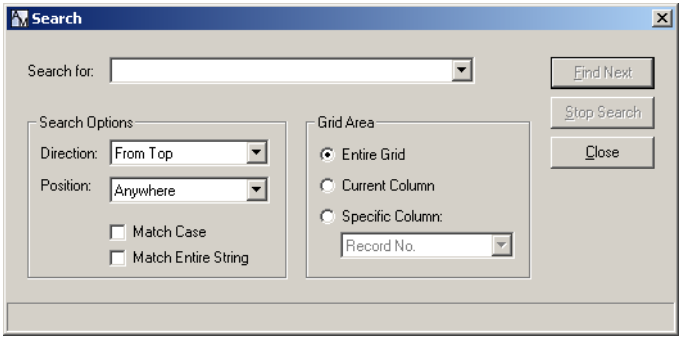
### ➤ To search audit records

1 Select and display a view file.

Run a query, if needed.

2 Select Tools ▸ Search.

The Search window appears. Also, if you have clicked in the audit record grid, the field you clicked is highlighted in blue as the current column and its row is highlighted in yellow.




3 In the Search field, enter a text string to find.

Your search entries are saved in the drop-down list for the current session.

4 If needed, use the Search Options to narrow your search.

- In the Direction drop-down list, select a direction to start the search. These include, From Top row down, the Next row down, and the Previous row down.
- In the Position drop-down list, select a search position. Select Anywhere or Beginning of cell, as appropriate.
- To match upper and lower case spellings, select the Match Case checkbox.
- To match the entire search string instead of just part of a cell, select the Match Entire String checkbox.

5 If needed, use the Grid Area to narrow your search.

- Select Entire Grid to search all columns.
- Select Current Column to search only the column selected, which is indicated as a blue field in the yellow highlighted field that you have clicked. If this column is not the one you want to set as the current column to search, close the Search window, click the desired column, and search again.
- Select Specific Column and select a column name from the drop-down list.

6 When you are ready, click Find Next.

Found items, if any, appear highlighted in the audit record grid. Otherwise, the status bar at the bottom of the Search window displays the message, “The text was not found.”

## Sorting Audit Records

Audit records can be sorted on up to three visible data fields. If needed, reset Visible Columns to add columns for sorting.

### ➢ To sort audit records

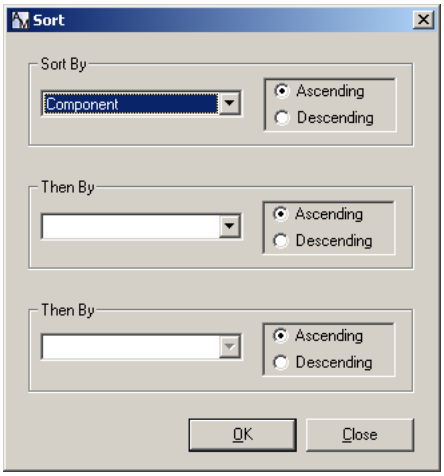
1. Select and display a current or archived view file.

   Run a query, if needed.

2. In the audit record grid, select a range of rows and columns.

3. Select Tools ▸ Sort.

   The Sort window appears.




4. In the Sort By drop-down list, select a column name.

   For example, User Name to order records alphabetically by user.

5. Select Ascending or Descending order for sorting.

   For example, if you are sorting by Time, to start the list with the most recent records, choose Descending.

6. To sort again using a second and third column, select from each Then By drop-down list, including Ascending or Descending.

7. Click OK.

   The audit record grid displays the sorted records.

## Exporting Audit Records to Other Applications

AuditMaster can export any query result to a comma- or tab-delimited text file for importing into other applications.

**Note** Only records and fields visible in the query result are exported.

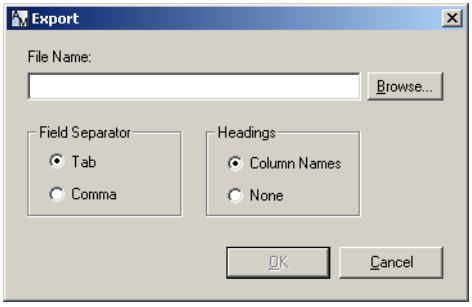
### ➤ To export audit records

1 Select and display a current view or archived file.

Run a query, if needed.

2 Select Tools ▸ Export.

The Export window appears.




3 Select tab- or comma-delimited fields for the exported columns.

4 To include column names in the text file, leave the default selected, otherwise select None.

5 Click OK to export the file to *filename*.txt.

The export file is saved to the location and name you provided.

**Note** You can also extract audit data directly by copying from the AuditMaster audit record grid and pasting the rows and columns into another application, such as a spreadsheet.

# Displaying Audit Records under Pervasive PSQL Security

If you run AuditMaster with Pervasive PSQL security enabled, field values in the User Name and Database Name columns vary with the DefaultDB database security policy and the type of database operation as shown in the following table.

*Table 7-5 User and Database Names Audited under DefaultDB Database Security*

| | Btrieve Operations | | SQL Engine Operations | |
|---|---|---|---|---|
| **Security Policy** | **User Name Displayed** | **Database Name Displayed** | **User Name Displayed** | **Database Name Displayed** |
| Database | Database login | One of the following:<br>• Database name from Btrieve Login API or connection string<br>• Database name bound to Btrieve file on which operation executed, if any<br>• "DefaultDB" if other two unavailable | Database login | n/a |
| Mixed | Database login | | Database login | n/a |
| Classic | • OS login<br>• Database user name if database security enabled | | • OS login<br>• Database user name if database security enabled | n/a |

Audited Btrieve operations include Select/Read, Insert, Update, Delete, Login, and Logout. For Begin Transaction, End Transaction, Abort Transaction, and Reset operations, which are not associated with a specific database, the database name is not available.

Login errors are listed with the invalid user name and/or database name. For SQL logins, the host name is not known at login time but afterward the host name becomes available and is displayed for SQL operations.

Under Mixed security, database logins match OS or network logins.

**Note** For more information on database operations in a Pervasive security environment, see the security chapter in Pervasive PSQL *Advanced Operations Guide*.

## Using AuditMaster Undo

On Windows platforms, the AuditMaster Undo command makes it possible to reverse certain database events. Successful results depend on the operation to be undone and the current state of the record involved, which may have changed again since the event occurred (e.g., unique indexing). In the case of updates to application data fields, the Before and After columns in the detail view identify what data value AuditMaster can attempt to restore to the Before state.

*Table 7-6 Results of Undo Command*

| Operation | Results of Undo |
|---|---|
| **Insert** | Deletes record, if it still exists and no other conditions stop insertion |
| **Delete** | Reinserts record if it does not exist, or if it does, so long as duplicates are allowed and no other conditions prohibit the insertion |
| **Update** | Restores Before state of record, if it still exists and no other conditions stop the update |

**Caution** Before attempting an undo, consider the following:

- The Windows user name under which you log in and open AuditMaster Viewer must have write permission for the Pervasive PSQL database being monitored. Neither Windows nor the Pervasive PSQL server recognize the administrator and regular user accounts created within AuditMaster.
- The file listed in the audit record must not have been removed from its audit configuration since the operation occurred.
- Undoing operations from within AuditMaster carries a risk of putting application data into an inconsistent or illogical state. You should be an advanced Pervasive PSQL user who understands the cautions regarding changing one part of an application database independently of another part.

- If files in an audit configuration group have the same name but different paths, undo applies only to the first file listed.

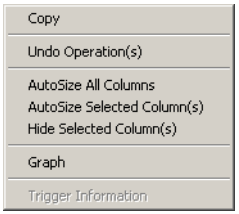
Note: Remote client logins do not support undo.

---

### ➢ To undo a database operation

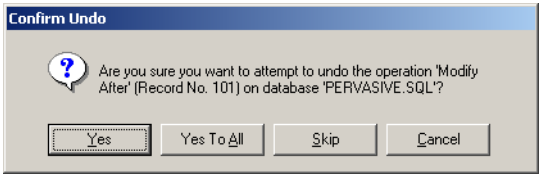
**1** In the audit record grid, right-click one or more records.

The shortcut menu appears.




**2** Select Undo Operation(s).

The system prompts you to confirm the undo attempt.


Confirm Undo
Are you sure you want to attempt to undo the operation 'Modify After' (Record No. 101) on database 'PERVASIVE.SQL'?
Yes
Yes To All
Skip
Cancel

**3** Click Yes, or Cancel if you change your mind.

If you selected multiple records to undo, you may select Yes to All to attempt to undo all of them without further interaction, or use the Skip and Yes buttons to work through them one at a time.

**Note** An undo operation is itself captured as an audit record and can be reversed by an additional undo.

---

chapter

# Administering AuditMaster

8

*A Walk-through of Administrative Tasks*

As an administrator, you will perform certain tasks to define how AuditMaster operates. As for adding audit configurations, the menu commands for these tasks are available only to users with administrative rights.

- Adding and Removing Servers
- Removing the Network Share
- Reviewing System Activity in the Status Log
- Maintaining Users
- Setting the Audit Filter
- Maintaining Server Settings

# Adding and Removing Servers

In AuditMaster, a server is a Pervasive PSQL server on which an AuditMaster event handler is running. The file amserver contains the server connection settings used by AuditMaster. This file is typically located on the server in the data folder of the AuditMaster installation directory.

This section provides instructions for the following topics:

- Adding a Server
- Editing the Server Description
- Removing a Server

## *Adding a Server*

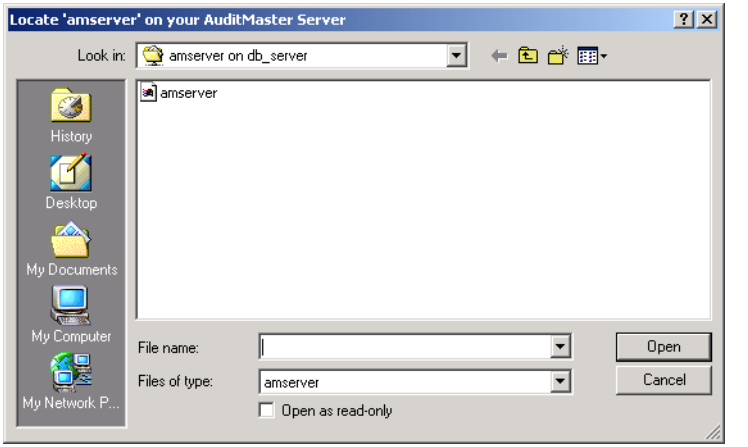
When you add an AuditMaster server, you enable the AuditMaster Viewer client to connect to an AuditMaster server either on the local machine or elsewhere on the network. You can add any AuditMaster server to which you have network access and file permissions.

### ➢ To add a server

1 Check the server machine you wish to add to make sure that Pervasive PSQL services are running. You may use Pervasive PSQL Control Center for this verification.

2 From AuditMaster Viewer, select Server ▸ Add.

The Locate 'amserver' on Your AuditMaster Server dialog box appears.

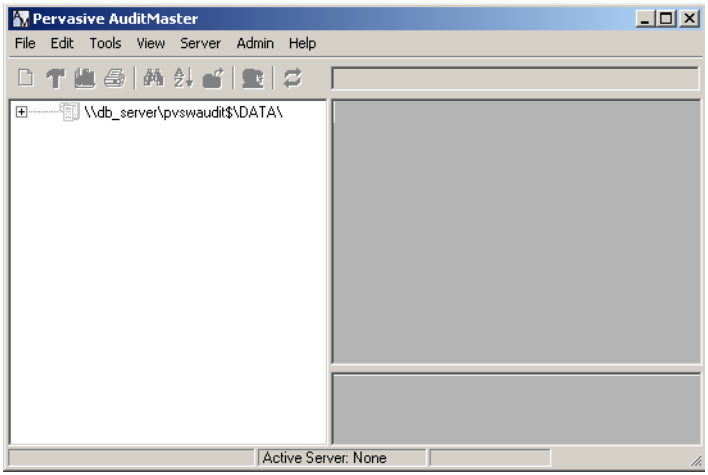


**3** Enter the path to the file amserver to read the settings for the AuditMaster server to which you want to a client connection.

This path is *server*\PVSWAUDIT$\DATA\amserver in a default installation, where *server* is the name of the Pervasive PSQL machine with the database to be monitored. Note that a share name other than PVSWAUDIT$ may have been chosen.

**4** Click Open.

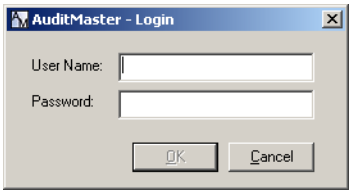
The server you selected is added to the list.




**Note** If your client is unable to connect successfully to the AuditMaster server, you may receive a –108 error message. The cause may be a faulty network mapping or other network problem. It may also involve a license key with too low a user count. See Authorization License.

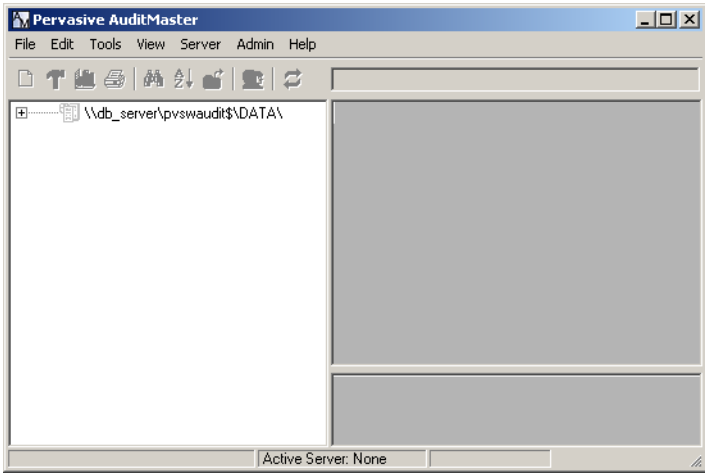
**5** Right-click a server configuration to select Login. You may also double-click.

The AuditMaster Login dialog box appears.




**6** Enter a valid user name and password, and click OK.

**Note** The built-in user ID admin has the default password MASTER. Passwords are case-sensitive; user names are not. To change this password, see Changing Your User Password. For information on the relation of AuditMaster logins to database and OS logins, read under Displaying Audit Records under Pervasive PSQL Security.




The new server is now ready for monitoring.

## *Editing the Server Description*

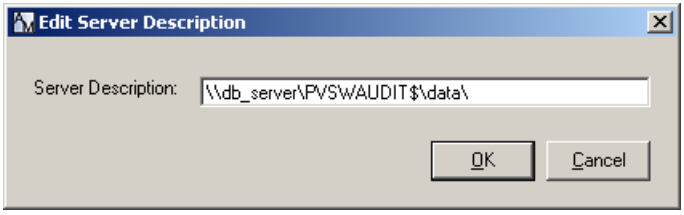
When a server is added for monitoring, its default name in the data tree uses the path name to the \Data folder in the AuditMaster home directory. If needed, you can assign a more meaningful name.

**Note** Data tree names have no effect on network names.

### ➤ To edit a server description

1 In the data tree, right-click the server icon and select Edit Server Description.

The Edit Server Description dialog box appears.




2 Replace the string with new text. You may use spaces.

3 Click OK.

The server icon in the data tree has a new name.

## *Removing a Server*

When you remove a server connection from an AuditMaster viewer client data tree, the client no longer has access to that server. However, auditing continues on the server, and existing audit records, users, and settings remain because the server is where they are stored. If you add the server connection again, everything that was present before is redisplayed in the data tree.

### ➤ To remove a server

1 Click a server in the AuditMaster data tree and select Server ▸ Remove.

A dialog box prompts you to confirm the removal.

2 Select Yes to remove the server.

The server is removed from the data tree.

## Removing the Network Share

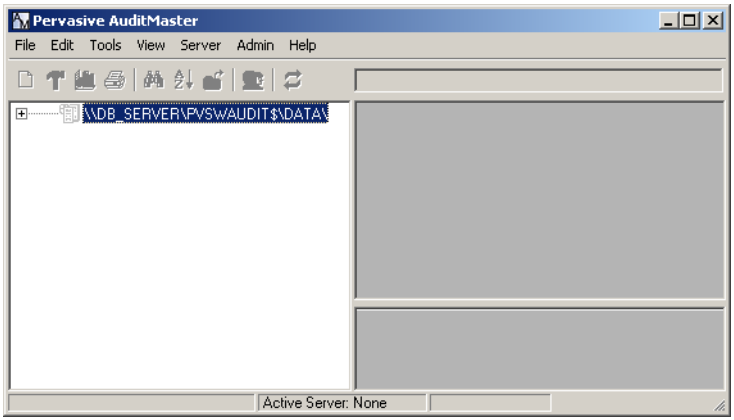
AuditMaster under Microsoft Windows installs a hidden network share to enable remote client access for AuditMaster Viewer from other machines. If you would like to disable the network share for security reasons, you can replace it with an explicit local path name after AuditMaster installation. This replacement can be done only on the server where AuditMaster is installed, not from a remote client. No existing audit records are affected, but auditing must stop momentarily when you restart the event handler to complete the share removal process.

**Note** Removing the network share will prevent remote access by all AuditMaster Viewer clients to the AuditMaster system. Be sure that you want to remove it.

### ➤ To replace the default network share with a local path name

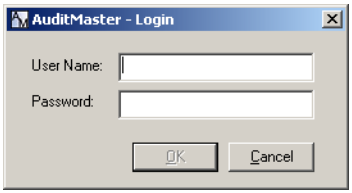
1 On the machine where AuditMaster server is installed, open AuditMaster Viewer from the operating system Start menu or Start screen.

The Pervasive AuditMaster window appears, listing servers available for monitoring.




2 Right-click a server configuration to select Login. You may also double-click.

The AuditMaster Login dialog box appears.

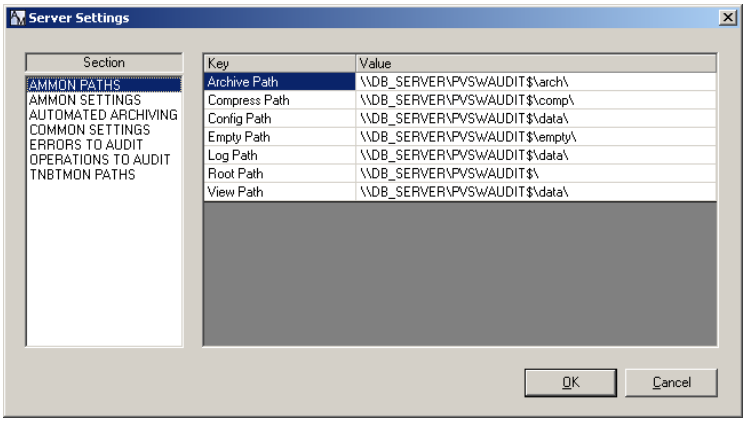



**3** Enter an AuditMaster administrative login name and password, and click OK.

**Note** The built-in user ID admin has the default password MASTER. Passwords are case-sensitive; user names are not. To change this password, see Changing Your User Password. For information on the relation of AuditMaster logins to database and OS logins, read under Displaying Audit Records under Pervasive PSQL Security.

**4** Select Admin ▸ Server Settings.

The Server Settings dialog box appears. On the left, the AMMON path settings are at the top of the list and are already highlighted.



**5** For each of the settings in the Value column on the right, double-click the path name and change

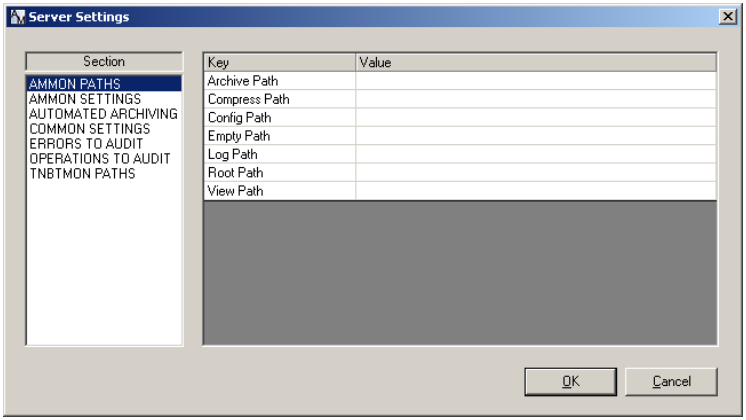
*server*\PVSWAUDIT$

to

*drive:\Pervasive PSQL root directory*\Audit

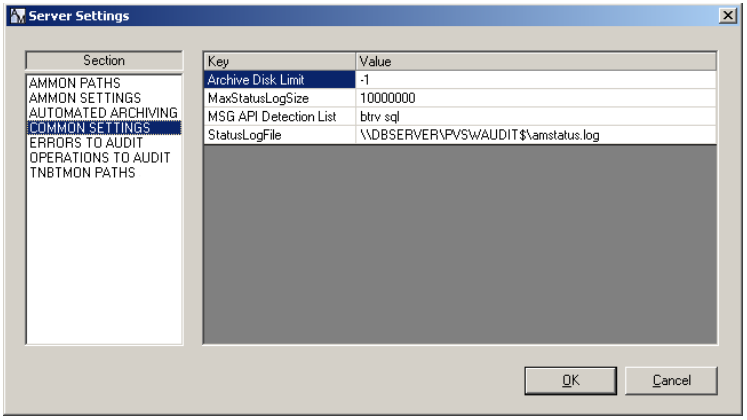
where *server* is the name of the machine on which Pervasive PSQL server and the AuditMaster event handler are installed and *drive* and *Pervasive PSQL root directory* are, respectively, the local drive letter and path name to the AuditMaster directory selected at installation time.

In this example, the result would resemble the following:



**6** In the list of sections on the left, select Common Settings.

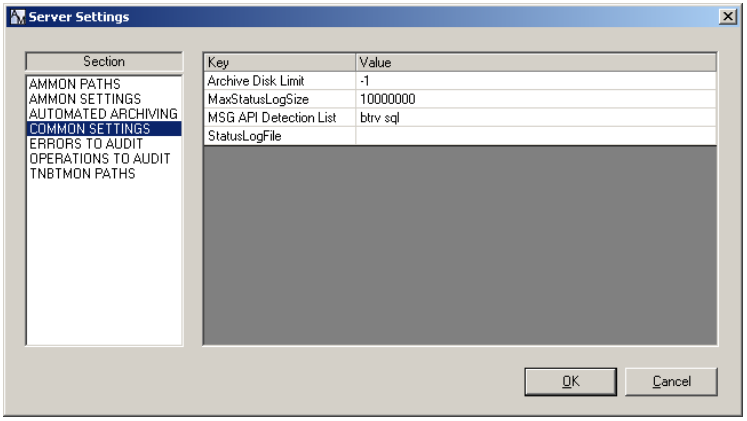
The dialog box displays the values on the right.




**7** Double-click the value for the AuditMaster status log file and change it to

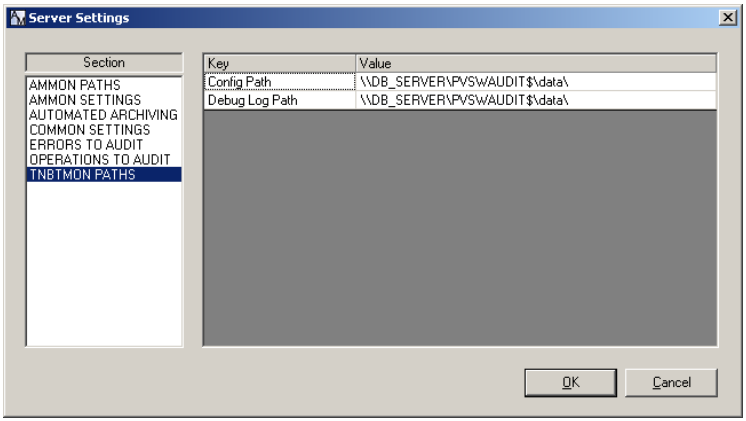
*drive:\Pervasive PSQL root directory*\Audit\amstatus.log

The result might resemble the following:



**8** In the list of sections on the left, select **TNBTMON Paths**.

The dialog box displays the values on the right.



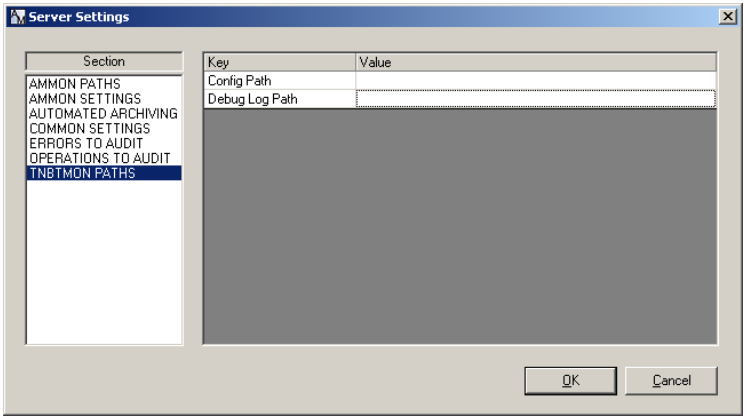

**9** Double-click the value for each path name and change

*server*\PVSWAudit$

to

*drive:\Pervasive PSQL root directory*\Audit

The result might resemble the following:



**10** After you have finished changing the values, click **OK**.

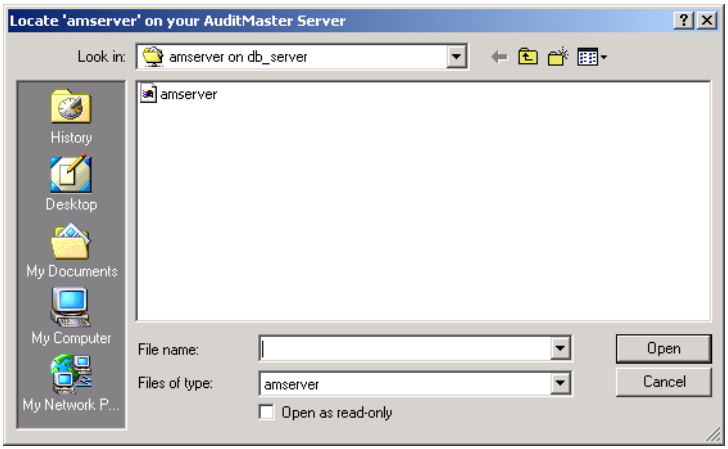
The system displays a prompt to restart the event handler.

**11** Click OK.

Do not restart the event handler yet. You will do that later in this task. If needed, see Restarting the AuditMaster Event Handler.

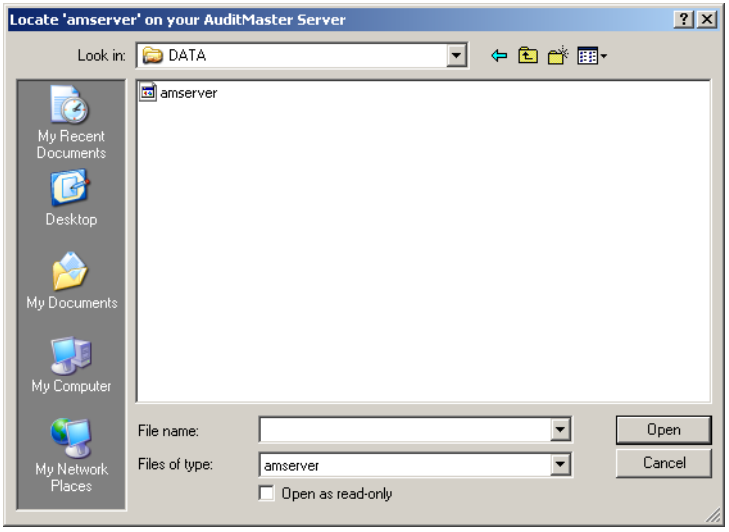
**12** Select Server ▸ Add.

The Locate 'amserver' on Your AuditMaster Server dialog box appears.



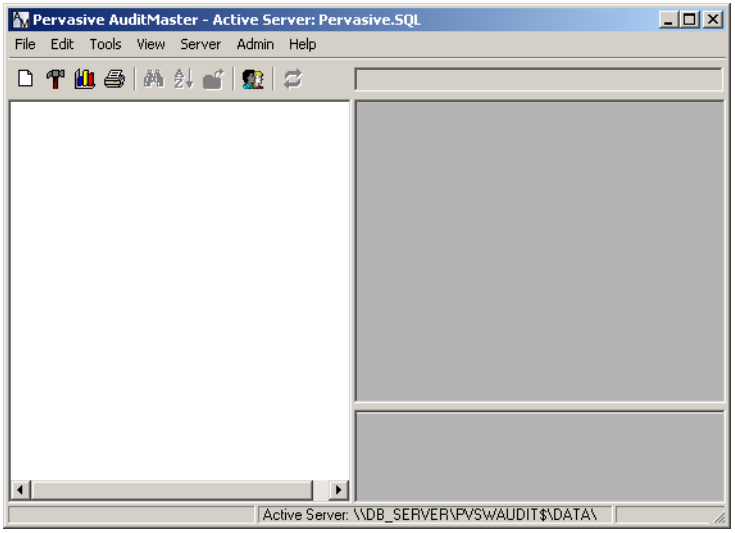

**13** Using the new path value that you have been implementing, enter *drive:\Pervasive PSQL root directory*\Audit\DATA to navigate to the location of the file amserver, which contains all of the settings you have just changed.

The path name you enter might resemble the following:



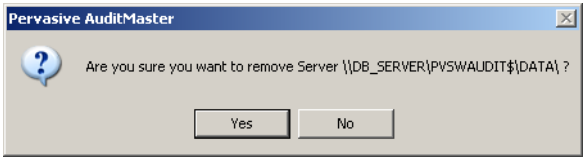

**14** Select the file amserver, and click Open.

Based on the new server settings you have entered, the new server appears.


Pervasive AuditMaster - Active Server: Pervasive.SQL
File Edit Tools View Server Admin Help
Active Server: \\DB_SERVER\PVSWAUDIT$\DATA\

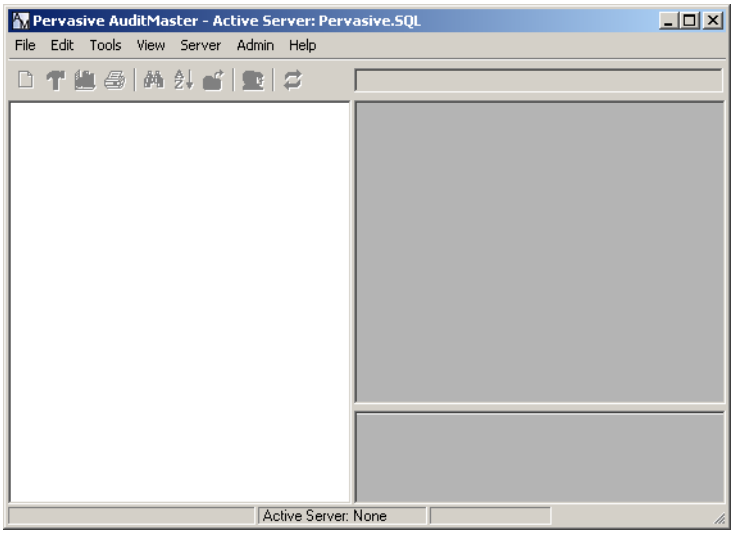
**15** Select the old server node with the network share in its name and then select Server ▸ Remove.

The system prompts you to confirm removal of the old server configuration.




**16** Click Yes.

The server is removed from the list and the status field at the bottom of the main window indicates no server is active.




**17** Exit from AuditMaster Viewer.

In order to remove the network share, AuditMaster and Pervasive PSQL services must not be running.

**18** If Pervasive PSQL Control Center (PCC) is not running, start it from the operating system Start menu or Start screen.

**19** In Pervasive PSQL Explorer, right-click the Services node and select Stop All Services.

**20** In Windows Explorer, open the folder *drive:\Pervasive PSQL root directory.*

The shared folder Audit appears in the list of files.

**21** Right-click the shared folder icon and select Properties.

The Properties window appears.

**22** Select the Sharing tab.

The Sharing pane comes to the front.

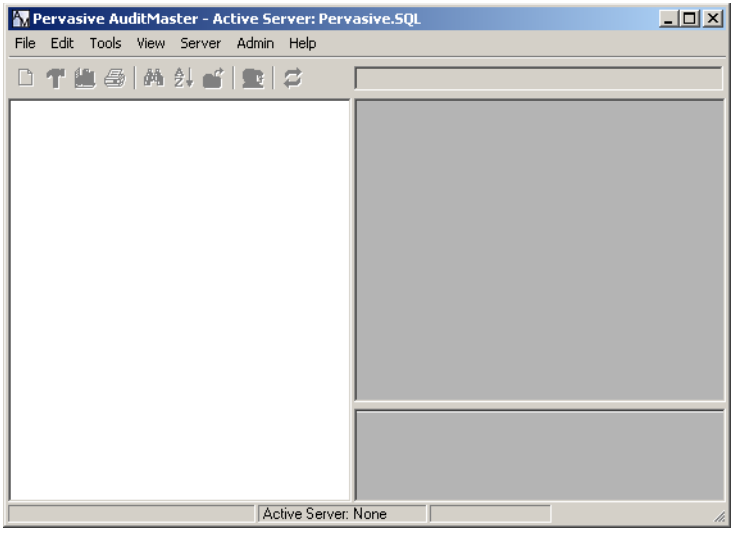
**23** Select Do not share this folder, and click OK.

The share is deleted and the Properties window closes.

**24** In Pervasive PSQL Explorer, right-click the Services node and select Start All Services.

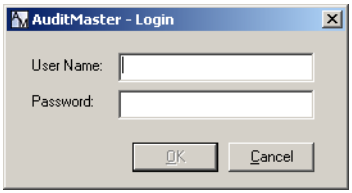
**25** After the services have restarted, verify that AuditMaster is working properly without a network share by opening the viewer to log in. Open AuditMaster Viewer from the operating system Start menu or Start screen.

The Pervasive AuditMaster window appears, showing the available server.



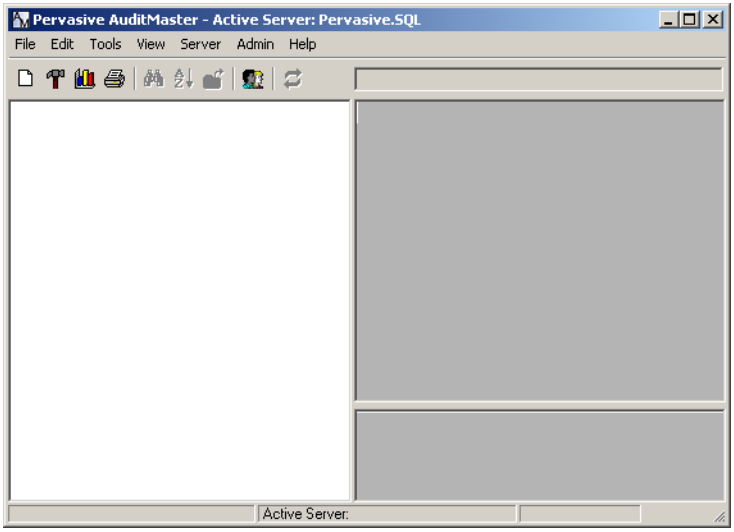

**26** Right-click the configuration to select Login. You may also double-click.

The AuditMaster Login dialog box appears.




**27** Enter an AuditMaster administrative user name and password, and click OK.

**Note** The built-in user ID admin has the default password MASTER. Passwords are case-sensitive; user names are not. To change this password, see Changing Your User Password. For information on the relation of AuditMaster logins to database and OS logins, read under Displaying Audit Records under Pervasive PSQL Security.




The new AuditMaster server is now ready to operate without a network share. Other server settings are unchanged and previously captured audit records captured remain in the system. Only the means of the viewer client connection has changed.

# Reviewing System Activity in the Status Log

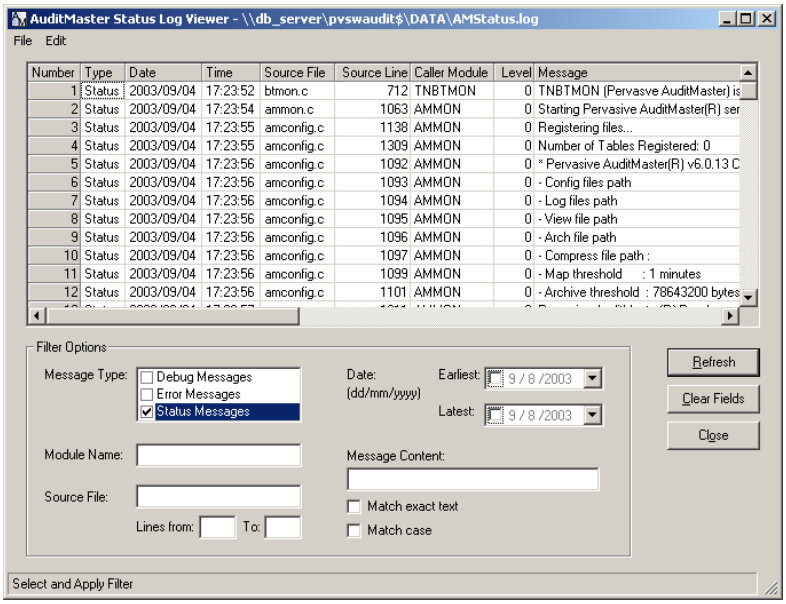
AuditMaster Status Log Viewer displays the activity logging that the system performs on itself. It provides a list of status messages and internal errors generated by AuditMaster operations. In a development environment, it also can be configured to capture messages for debugging purposes.

### ➤ To view, filter, and sort status log records

**1** Open Status Log Viewer by doing one of the following:

- In AuditMaster Viewer, select Admin then View Status Log.
- Access the Status Log from operating system Start menu or Apps screen, or from the installation location (the default is C:\<*installation directory*>\Audit\Data). This method is especially useful if the viewer is not responding because of a system problem, such as disk full.

The Status Log Viewer window displays several types of messages. Normally, these are all status messages to provide information on current system operation.


AuditMaster Status Log Viewer - \\db_server\pvswaudit$\DATA\AMStatus.log
File Edit
Number Type Date Time Source File Source Line Caller Module Level Message
1 Status 2003/09/04 17:23:52 btmon.c 712 TNBTMON 0 TNBTMON (Pervasve AuditMaster) is
2 Status 2003/09/04 17:23:54 ammon.c 1063 AMMON 0 Starting Pervasive AuditMaster(R) ser
3 Status 2003/09/04 17:23:55 amconfig.c 1138 AMMON 0 Registering files...
4 Status 2003/09/04 17:23:55 amconfig.c 1309 AMMON 0 Number of Tables Registered: 0
5 Status 2003/09/04 17:23:56 amconfig.c 1092 AMMON 0 * Pervasive AuditMaster(R) v6.0.13 C
6 Status 2003/09/04 17:23:56 amconfig.c 1093 AMMON 0 - Config files path
7 Status 2003/09/04 17:23:56 amconfig.c 1094 AMMON 0 - Log files path
8 Status 2003/09/04 17:23:56 amconfig.c 1095 AMMON 0 - View file path
9 Status 2003/09/04 17:23:56 amconfig.c 1096 AMMON 0 - Arch file path
10 Status 2003/09/04 17:23:56 amconfig.c 1097 AMMON 0 - Compress file path :
11 Status 2003/09/04 17:23:56 amconfig.c 1099 AMMON 0 - Map threshold : 1 minutes
12 Status 2003/09/04 17:23:56 amconfig.c 1101 AMMON 0 - Archive threshold : 78643200 bytes
Filter Options
Message Type:
Debug Messages
Error Messages
Status Messages
Date: (dd/mm/yyyy)
Earliest: 9 / 8 /2003
Latest: 9 / 8 /2003
Refresh
Clear Fields
Close
Module Name:
Message Content:
Source File:
Match exact text
Lines from:
To:
Match case
Select and Apply Filter

2 If needed, set filter options to display only the status records you want. The Clear Fields button allows you to start over on most fields. The filtering options are given in the following list:

- To filter the log by the type of message, select the type of message from the Message Type list.
- You may choose to view debug and error messages, which can be helpful in troubleshooting any unexpected behavior in AuditMaster.
- To filter by the Module Name, enter the name of the module.
- To filter by the source file, enter the name of the source file.
- You can look at specific lines of the source file by entering the line numbers in the fields provided.
- To filter by specific dates, select dates from the Earliest and Latest lists.
- To filter by searching for message content, enter a text string and select checkboxes for matching exact text or case.

  For example, the text string `archiv` will display only status records related to AuditMaster archived files.

  Selecting for exact text requires that the Message Content field contain the entire text string for the search. If you are searching for partial text strings, leave this checkbox cleared.

3 When you are finished setting filter options, click Refresh.

The viewer refreshes with only records you wish to see.

4 You also may sort status log records by selecting column headers on which to sort.

For example, use the SHIFT key to select both the Date and Time columns to order the records chronologically.

5 After selecting columns on which to sort, click Refresh.

The viewer refreshes by sorting the records displayed.

# Maintaining Users

As part of AuditMaster security, only trusted personnel are allowed access to the AuditMaster system. As administrator, you must define user names and provide a password for each user. You must also decide whether each user shall also have your same administrator privileges.

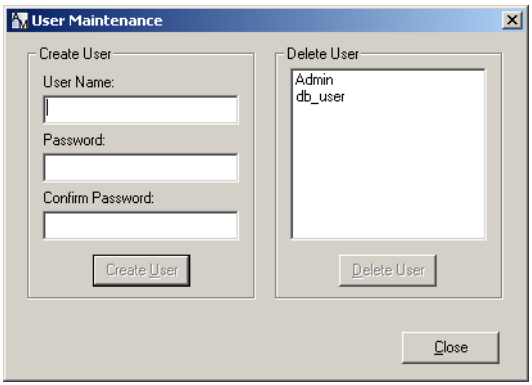
This section covers tasks done in the User Maintenance window.

- To add a user
- To remove a user

## ➤ To add a user

**1** Select Admin ▸ User Maintenance.

The User Maintenance window appears.




**2** Enter a user name and password. Passwords are case-sensitive, user names are not.

**3** Click Create User.

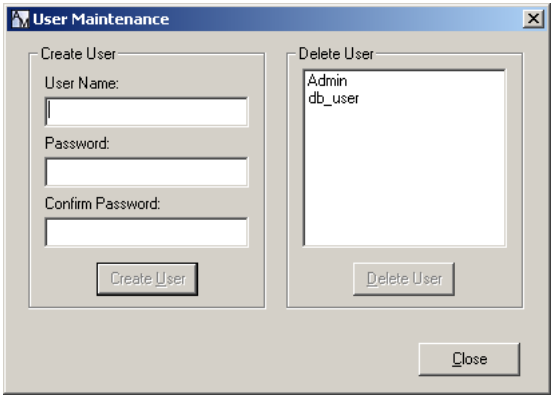
**4** You are asked whether this user is to have AuditMaster administrator privileges. Click Yes or No as appropriate.

The new user appears in the list of current users.

### ➤ To remove a user

1 Select Admin ▸ User Maintenance.

The User Maintenance window appears.




2 Select a user in the Delete User list.

3 Click Delete User.

4 You are asked to confirm the deletion. Click OK.

The user is removed from the list.

## Setting the Audit Filter

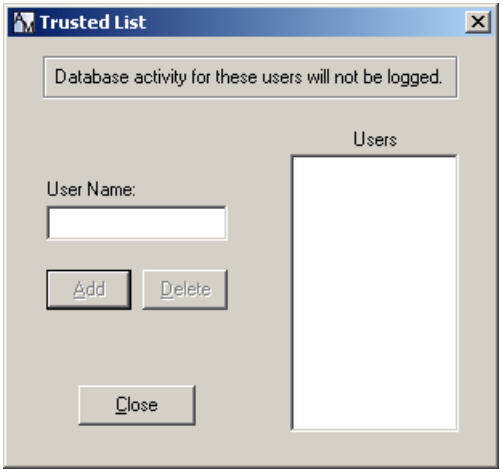
The trusted list restricts auditing by stopping capture of audit records of low value, such as monitoring of system or batch processes that represent no direct access by human users.

Once a name is listed as trusted, the system ignores it globally and logs no activity for that name for any audit configuration.

### ➤ To add a name to the trusted list

1 Select the Admin ▸ Audit Filter ▸ Trusted List command.

The Trusted List window appears.




2 In the User Name field, enter a text string as it would appear in the User Name column of the audit record grid. The string you enter is not case-sensitive (i.e., SYSTEM, System, and system are the same).

The Add button becomes active.

3 Click the Add button.

The name you entered moves to the Users list.

4 Click Close.

5 To activate the new trusted list, you must restart the event handler. See Restarting the AuditMaster Event Handler.

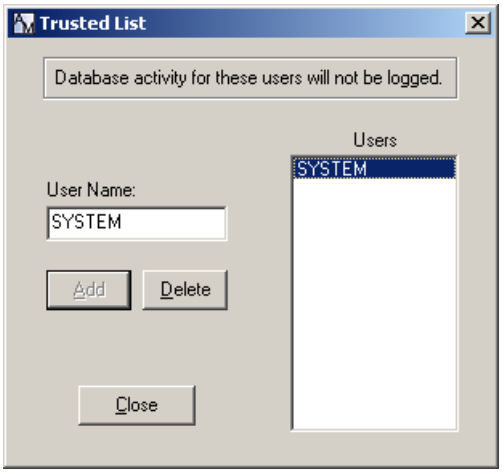
### ➢ To delete a name from the Trusted List

1 Select the Admin ▸ Audit Filter ▸ Trusted List command.

The Trusted List window appears.

2 In the Users field, select one or more names to delete. You may use shift-click and control-click for your selection.

The Delete button becomes active.




3 Click the Delete button.

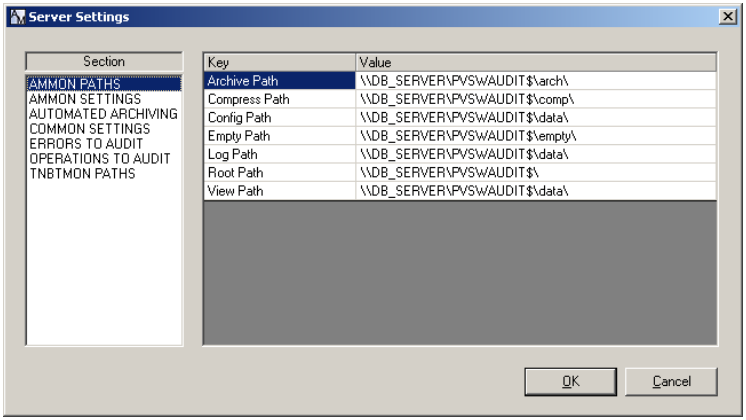
Your selections are removed from the trusted list.

4 Click Close.

5 To activate the new trusted list, you must restart the event handler. See Restarting the AuditMaster Event Handler.

## Maintaining Server Settings

The Server Settings window displays AuditMaster system settings. It is available using the Admin ▸ Server Settings command.




The window offers the following sections of system settings:

- Ammon Paths
- Ammon Settings
- Automated Archiving
- Common Settings
- Errors to Audit
- Operations to Audit
- TNBTMON Paths

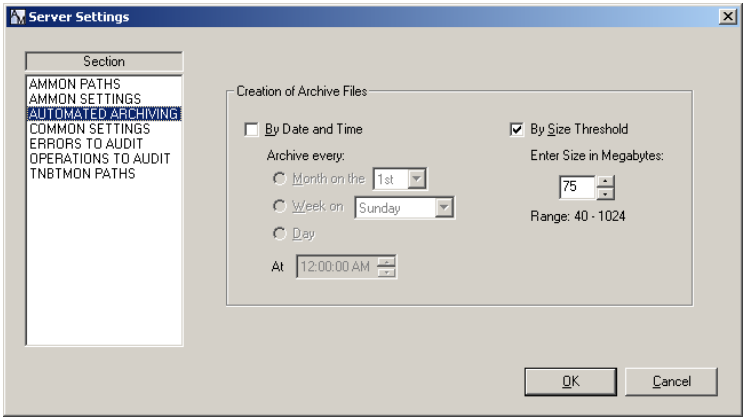
Some of the settings in these sections can be changed; however, in most cases it is best to leave the defaults, with the possible exception of the following options:

- Automated Archiving
- Archives to Keep
- Archive Disk Limit
- Errors to Audit
- Operations to Audit Globally

After a change is made, except for automated archiving, the event handler must restart to activate the new setting. If needed, see Restarting the AuditMaster Event Handler.

## *Automated Archiving*

The Automated Archiving section offers options for configuring the audit record archiving.



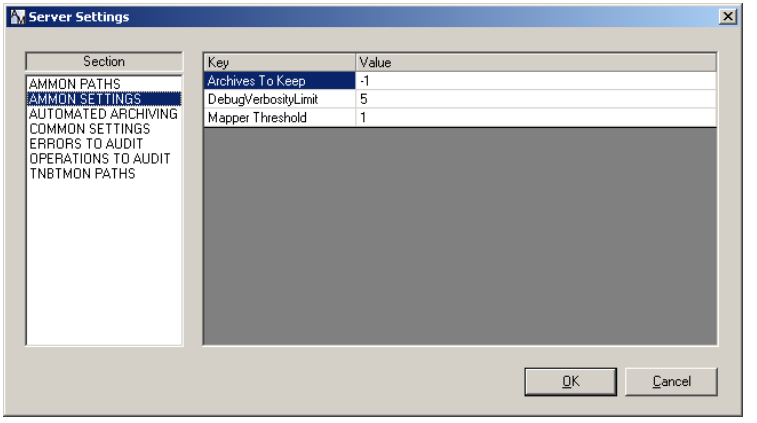

By default, AuditMaster automatically moves audit records to an archived file when audit records in the log file reach 75 MB. However, in the Automated Archiving section of Server Settings, you can change this default size, choose to archive by date, or a combination of the two.

If you select the checkboxes for both By Date and Time and By Size Threshold, then whichever condition occurs first will prompt the system to create an archived file and reset the log file to empty.

If you clear the By Size Threshold setting and choose only By Date and Time, the system still uses a 2 GB size threshold. If the date and time you select has not occurred and the log file size reaches 2 GB, the system will automatically archive, then when the date and time arrive, it will archive again.

### *Archives to Keep*

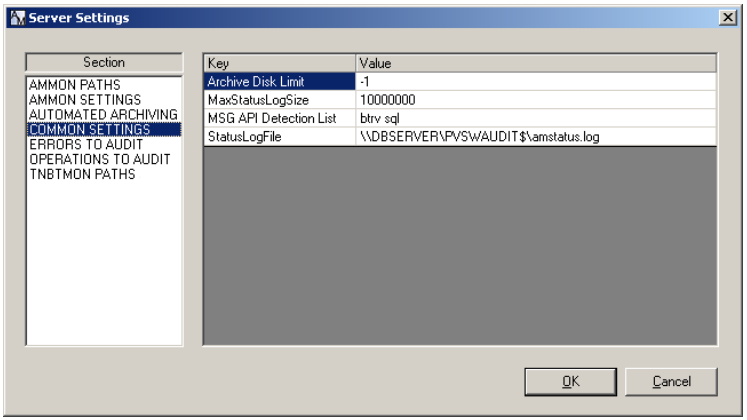
The Ammon Settings section offers one settable value, Archives to Keep. By default, the value is –1, which means that the system does not monitor the number of archived files. If the value is greater than zero, then the system retains only that number of the most recent files and deletes the older ones.




**Caution** Use of this setting may lead to unintentional loss of archived audit records. Be sure to consider the possible situations when it may be undesirable to delete archived files automatically.

### *Archive Disk Limit*

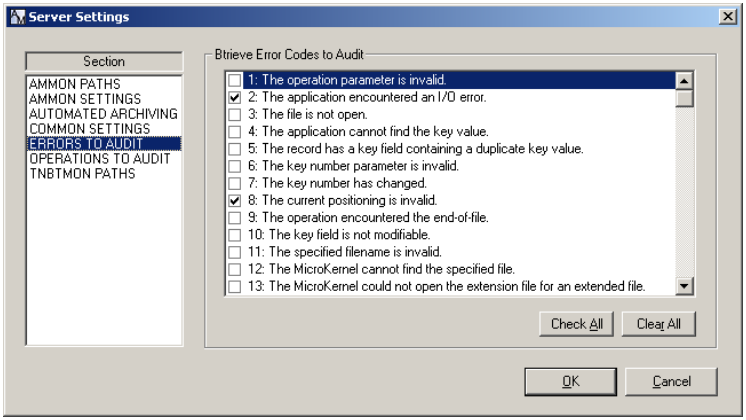
The Common Settings section offers one settable value, Archive Disk Limit. By default, the value is –1, which means that the system does not monitor the total size of all archived files. If the value is greater than zero bytes, then the system retains only the most recent files for which the total size is less than or equal to this number of bytes and deletes the older files.




**Caution** Use of this setting may lead to unintentional loss of archived audit records. Be sure to consider the possible situations when it may be undesirable to delete archived files automatically.

## Errors to Audit

The Errors to Audit section sets the Pervasive PSQL status codes to log as audit events.


Server Settings
Section
AMMON PATHS
AMMON SETTINGS
AUTOMATED ARCHIVING
COMMON SETTINGS
ERRORS TO AUDIT
OPERATIONS TO AUDIT
TNBTMON PATHS
Btrieve Error Codes to Audit
1: The operation parameter is invalid.
2: The application encountered an I/O error.
3: The file is not open.
4: The application cannot find the key value.
5: The record has a key field containing a duplicate key value.
6: The key number parameter is invalid.
7: The key number has changed.
8: The current positioning is invalid.
9: The operation encountered the end-of-file.
10: The key field is not modifiable.
11: The specified filename is invalid.
12: The MicroKernel cannot find the specified file.
13: The MicroKernel could not open the extension file for an extended file.
Check All
Clear All
OK
Cancel

After AuditMaster installation, the default settings are as follows:

*Table 8-1 Default Errors to Audit after AuditMaster Installation*

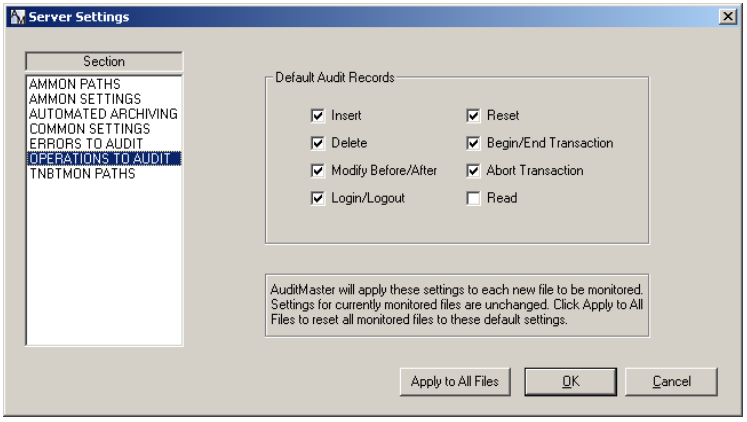
| Error | Description |
|---|---|
| 2 | The application encountered an I/O error. |
| 8 | The current positioning is invalid. |
| 18 | The disk is full. |
| 19 | The application encountered an unrecoverable error. |
| 32 | The file cannot be extended. |
| 37 | Another transaction is active. |
| 43 | The specified record address is invalid. |
| 46 | Access to the specified file is denied. |
| 51 | The owner name is invalid. |
| 54 | The variable-length portion of the record is corrupt. |
| 67 | The MicroKernel cannot open the SQL data dictionary files. |
| 69 | The Delete operation specified a file that is damaged. |
| 73 | The RI definition is out of sync. |
| 101 | Insufficient operating system memory is available. |

*Table 8-1 Default Errors to Audit after AuditMaster Installation*

| Error | Description |
|---|---|
| 138 | The MicroKernel has detected an invalid null indicator. |
| 141 | The user name is invalid for the database login. |
| 142 | The database specified on login is invalid. |
| 143 | The MicroKernel cannot allow unauthorized access to files in a secure database. |
| 147 | The log segment is missing. |
| 148 | A roll forward error occurred. |

## Operations to Audit Globally

The Operations to Audit window offers the same type of settings as the Operations to Audit button in the Audit Configuration window.




The difference is that in Server Settings the options are global for any file selected in an audit configuration, and in the Audit Configuration window, the button allows you to set operations to audit for individual files.

At installation time, the AuditMaster defaults in this window include all operations except Read. If you select different options, they become the new defaults for any file you add to an audit configuration group. Operations to audit set for earlier added files are not affected unless you click the Apply to All Files button.

Finally, if any file is removed from a group and then added again, its operations to audit settings default to the current selections in this window.

For information on individual file settings, see Operations to Audit by File.

**Note** In a Pervasive PSQL database, when the client-side cache engine is turned on, the cache engine reads an entire database page after 8 consecutive reads in anticipation of more reads. The records in the database page read by the cache engine are not audited by the event handler on the server. If auditing requires that every read be captured, verify the setting is off. However, lack of engine caching can reduce database performance. The behavior occurs only when the threshold of 8 consecutive reads is reached. If 7 reads and then an update occurs, no caching occurs and all 7 reads are captured. In Pervasive PSQL Control Center, expand Local Client, right-click MicroKernel Router, and select Properties, then click Performance tuning to see the setting Use Cache Engine. By default, the setting is off.

appendix

A

# Basic Troubleshooting

*How to Identify and Solve Common Problems*

The topics in this chapter help you resolve common problems that you may encounter using AuditMaster.


- General Tips
- Troubleshooting Strategies
- Restarting the Status Log
- Handling Errors Relating to Paths
- No Records Returned by Query Despite Changes to Application Data
- Network Communications
- Database Engine
- How to Get Additional Help

## General Tips

This section lists general tips for using AuditMaster.

- When configuring your application data for monitoring, be sure that the files you select reside on the same server as the AuditMaster server.
- Be sure that the Pervasive settings are optimized. Common settings are communication protocols, files, and file handles. Check Pervasive documentation for information on configuration and optimization.
- AuditMaster numbers audit records automatically up to a 32-bit upper limit of 2,147,483,647. After that, numbering wraps and the next audit record starts again at 1. If you notice that the audit record number has suddenly dropped, check to see whether this has occurred.

## Troubleshooting Strategies

You must first diagnose a problem before you can fix it. The following checklist contains items to help you diagnose problems with AuditMaster.

- ❑ Does the AuditMaster status log contain errors? See Reviewing System Activity in the Status Log.
- ❑ Does the network function correctly? See Network Communications.
- ❑ Is the database engine running? See Database Engine.
- ❑ Are other sources of help available? See How to Get Additional Help.

## Restarting the Status Log

AuditMaster writes status records in the file amstatus.log, located in a default installation under C:\<*installation directory*>\Audit\Data. Under certain conditions, such as disk full, AuditMaster may be unable to continue adding status records into this file, even after the error condition is corrected. To restart the status log, you can export its contents and then delete the log. AuditMaster then starts a new log file automatically.

### ➤ To restart the status log

1. In the viewer window, select Admin ▸ View Status Log to open AuditMaster Status Log Viewer.
2. Select File ▸ Save As and give the status record text file a descriptive name.

   The status records are exported to a file with the suffix .txt and can be opened by applications that read text.
3. Exit from AuditMaster.
4. Stop the event handler.
5. Delete the original amstatus.log file from the \Data folder in the AuditMaster installation directory.
6. Restart the event handler.
7. AuditMaster status logging is now active again.

## Handling Errors Relating to Paths

### ➢ To verify correct path settings

1. Select Admin ▸ Server Settings.
2. Select AMMON PATHS.
3. Ensure that path points to directory where AuditMaster was installed.
4. In order for AuditMaster Viewer clients from remote machines to access the configuration, UNC paths must be specified. The default subdirectories are as follows:

*Table A-1 UNC Path Settings for Remote AuditMaster Viewer Clients*

| AMMON Path | UNC Path |
|---|---|
| Root | *server**amdir*\ |
| Config | *server**amdir*\data\ |
| Log | *server**amdir*\data\ |
| View | *server**amdir*\data\ |
| Archive | *server**amdir*\arch\ |
| Compress | *server**amdir*\comp\ |
| Empty | *server**amdir*\empty\ |

5. Verify the following information:
   - *Server* is the computer name where the AuditMaster event handler is installed.
   - *Amdir* is the path name that represents the directory where AuditMaster was installed.
   - Config Path, Log Path, and View Path should all be set to *server**amdir*\data\.
   - If the paths were not initialized properly during install, they should be set to *server**amdir*\...

## No Records Returned by Query Despite Changes to Application Data

1. Be sure the AuditMaster event handler is enabled.
   - The event handler can be enabled from the viewer by right-clicking on the monitor name under the Active Monitors node in the data tree.
   - The Pervasive PSQL database engine must be running in order for a monitor to be enabled or disabled.
   - Once the event handler has been enabled, the database engine must be restarted for auditing to start.
2. Check that the application files have been set for monitoring in an audit configuration.
3. If the event handler is enabled and the files have been configured, be sure to update the view file before querying.
4. Review the query to check that it is not so narrow that the result is no record.
5. Check the audit filter to make sure the trusted list is not preventing audit records from being captured.
6. Check that archiving has not just occurred, meaning that records of interest are no longer in the empty log file.
7. Check both AuditMaster and Pervasive licenses for activation or expiration.

# Network Communications

Pervasive System Analyzer (PSA) is a diagnostic utility included with the Pervasive PSQL database engines. PSA can be used as a stand-alone diagnostic tool to help you troubleshoot network problems.

**Note** For AuditMaster, use PSA only to troubleshoot network problems. PSA is capable of other functions pertaining only to the Pervasive PSQL database engines. The additional functions in PSA (such as archiving) do not apply to AuditMaster.

## *How to Start PSA*

➤ **To start PSA**

1 Access Pervasive System Analyzer from the operating system Start menu or Apps screen.

**Note** To troubleshoot your network communications for AuditMaster, select Test Active Installation on the System Analyzer Options dialog in PSA.

## *Documentation for PSA*

The use of PSA is detailed in the *Pervasive PSQL User's Guide*. Please see that guide for complete information regarding PSA.

## Database Engine

The Pervasive PSQL database engine must be running to perform replication.

### ➤ To verify Pervasive PSQL Server engine is running

1. Open the Services management console at the operating system.

   Refer to the operating system documentation for “services.”

2. Type ‘P’ or scroll the list of services until you reach the following services.

   - Pervasive.SQL (transactional)
   - Pervasive.SQL (relational)

   Both of these services must be started for the Pervasive PSQL database engine to function correctly.

   The Status column displays whether or not the service is currently running. The Startup column indicates whether the service is set to automatically start on system startup or start manually.

3. If a service is not started, select it in the list and click Start.

## How to Get Additional Help

Pervasive Software strives to ensure that your product installation is easy and successful. If you encounter problems during or after the installation that are not covered in the user documentation, please contact Pervasive Software and we will address your problem promptly.

The following table lists a variety of resources to help you get answers to your questions, troubleshoot problems, and interact with the Pervasive team as well as with other customers.

*Table A-2 Pervasive Software Resources*

| Resource | Description | Contact Information |
|---|---|---|
| Pervasive PSQL Web site | The site is a great source for everything Pervasive PSQL, such as the following:<br>• Product downloads for Pervasive PSQL, Pervasive AuditMaster, Pervasive Backup Agent, and Pervasive DataExchange<br>• Technical support and Knowledge Base<br>• Discussion forums<br>• Software development kit (SDK) downloads<br>• Product documentation, white papers, and technical papers<br>• Component downloads such as tools, solutions, and code samples<br>• Company contacts, and more! | http://www.pervasivedb.com |
| Pervasive PSQL FTP Site | An FTP site is available to upload files that you want to provide Technical Support | ftp://ftpsupport.pervasive.com |
| Pervasive PSQL Newsgroup | The Pervasive PSQL newsgroup is managed by the end-user community, posting and answering questions as they wish.<br>Note that the discussion forums on the Pervasive PSQL Web site have largely replaced activity on the newsgroup. | news://comp.databases.btrieve |
| Pervasive PSQL Printed Documentation | Printed versions of each manual are available for purchase separately, or you may purchase the entire documentation set. | E-mail database@pervasive.com<br>or telephone 1 800 287 4383. |

### *Technical Support*

If you still have questions or problems relating to your Pervasive AuditMaster installation, you can obtain help from the Pervasive Software Customer Support department.

appendix

# Advanced Operations

B

*Features for Power Users and Programmers*

This advanced operations chapter is for power users and programmers who need utilities and methods for accessing audit system beyond what is offered in AuditMaster Viewer.


- Managing Schemas from the Command Line
- Querying Audit Data Directly through SQL
- Using the Delta Alert Utility

## Managing Schemas from the Command Line

AuditMaster Schema Maintenance Wizard has a command-line version amschemamaint.exe, located under <*installation directory*>\Audit\Bin in a default installation. The AuditMaster installation calls this utility to create the Pervasive PSQL Demo and Pervasive PSQL Generic audit configurations by importing the following two files from the Schema folder in the install image root:

- Pervasive.SQL_Demo_V9.add
- Pervasive.SQL_Generic.add

In third-party applications, amschemamaint.exe can be used in scripts to export a schema to a file in the \Schema folder on a custom CD-ROM to automate its importing at installation time. The sequence of usage would be as follows:

1. Install your application.
2. Install AuditMaster.
3. Run amschemamaint.exe to import from the \Schema folder.

**Note** If you use amschemamaint.exe to customize an installation CD-ROM and wish to delete Pervasive.SQL_Demo_V9.add so that it does not appear in the Audit Configuration window, you may do so. However, do not remove Pervasive.SQL_Generic.add, since it is needed for successful operation of AuditMaster.

The amschemamaint.exe utility has four forms:

- import
- export
- remove
- list

Each of these is explained in the rest of this section.

## *import*

AuditMaster Schema Maintenance import utility.

### *Description*

Imports a schema from a Pervasive PSQL database or from a file. See export for steps to create .add files for importing.

### *Syntax*

Database: `amschemamaint import -d` *database_path* [`-m` *password*] -p "*product name*" `-v` *version* `-s` *description* [`-a` *folder*]

File: `amschemamaint import -i` *file_path_name* [`-a` *folder*]

### *Options*

| Option | Description |
|---|---|
| -a | Data directory on remote server where AuditMaster amserver file resides. Optional if amserver resides on the same machine as the client. |
| -d | Path name of database schema (.ddf files) to import |
| -m | Master password if database is secure |
| -p | Name of application to which the data belongs, for Product Name field in Audit Configuration window. With spaces, use quotation marks. |
| -s | Further description of product, for Product Description field of Audit Configuration window. |
| -v | Version number of the application to which the data belongs, for Version field in Audit Configuration window. |
| -i | Path and file name from which to import |
| -h | Help |

### *Example*

```
C:\>amschemamaint import -d d:\<installation
directory>\demodata -p "Pervasive PSQL Demo" -v 10.0 -s
"Pervasive PSQL Demonstration Data" -a
\\server_name\volume_name\data
```

## *export*

AuditMaster Schema Maintenance export utility.

### *Description*

Exports a schema from a Pervasive PSQL database to a file for later importing into AuditMaster.

### *Syntax*

`amschemamaint export -d` *database_path* [`-m` *password*] -p "*product name*" `-v` *version* `-s "`*description*`" -e` *file_path_name*

### *Options*

| Option | Description |
|---|---|
| -d | Path name of database schema (.ddf files) to import |
| -m | Master password if database is secure |
| -p | Name of application to which the data belongs, for Product Name field in Audit Configuration window. With spaces, use quotation marks. |
| -s | Further description of product, for Product Description field of Audit Configuration window. |
| -v | Version number of the application to which the data belongs, for Version field in Audit Configuration window. |
| -e | Path and file name to which to export |
| -h | Help |

### *Example*

```
C:\>amschemamaint export -d d:\<installation
directory>\demodata -p "Pervasive PSQL Demo" -v 10.0 -s
"Pervasive PSQL Demonstration Data" -e d:\<installation
directory>\demodata\auditschema
```

## *remove*

AuditMaster Schema Maintenance remove utility.

### *Description*

Removes a schema from the AuditMaster system.

### *Syntax*

`amschemamaint remove -p "`*product name*`" -v` *version* [`-a` *folder*]

### *Options*

| Option | Description |
|---|---|
| -a | Data directory on remote server where AuditMaster amserver file resides. Optional if amserver resides on the same machine as the client. |
| -p | Name of application to which the data belongs, for Product Name field in Audit Configuration window. With spaces, use quotation marks. |
| -v | Version number of the application to which the data belongs, for Version field in Audit Configuration window. |
| -h | Help |

### *Example*

```
C:\>amschemamaint remove -p "Pervasive PSQL Demo" -v
10.0 -a d:\data\audit
```

## list

AuditMaster Schema Maintenance list utility.

### Description

Displays all schemas currently in the audit configuration.

### Syntax

`amschemamaint list` [`-a` *folder*]

### Options

| Option | Description |
|---|---|
| -a | Data directory on remote server where AuditMaster amserver file resides. Optional if amserver resides on the same machine as the client. |
| -h | Help |

### Example

```
C:\>amschemamaint list
Current schema configurations:
Pervasive PSQL Generic [<default version>]
Pervasive PSQL Demo [10.0]
Pervasive PSQL Demo [10]
Pvideo [1.0]

C:\>amschemamaint list -a \\server_name\volume_name\audit\data
Current schema configurations:
Pervasive PSQL Generic [<default version>]
Pervasive PSQL Demo [10.0]
Pervasive PSQL Demo [10]
Pvideo [1.0]
```

# Querying Audit Data Directly through SQL

The AuditMaster Viewer client and its query builder are not the only means of access to audit records. You also can run direct SQL queries against audit records. To do so, you must first use the Query Data-Model Generator (QDMG) utility provided with AuditMaster. The utility generates a script to create a virtual database of views linked to audit records in the AuditMaster system.

Both current view and archived audit records can be queried directly using the query data-model method. Direct queries can support applications to create reports or otherwise display audit records, as well as serve development and debugging purposes.

Use cases are provided to demonstrate how to apply the direct query method to the Demodata database included in the Pervasive PSQL installation.

This section covers the following topics:


- Query Data-Model Generator Utility
- Creating a Virtual Database
- The Structure of an Audit Record
- Running a Query on the Current View File
- Running a Query on an Archived File
- Summary of Direct Query Methods

## Query Data-Model Generator Utility

Query Data-Model Generator utility for Pervasive AuditMaster.

### Description

Generates a script, consisting of a set of SQL statements, to run against an empty database. The script populates this virtual database with views that link to audit records stored in the AuditMaster log file. Once the views are created, you can then run queries against them to return results from audit records within AuditMaster.

### Syntax

`qdmg -d` *DDF_path* [`-m` *password*] `-p` *name* `-o` *file* [`-l` *logfile*] [`-a` *folder*]

### Options

| Option | Description |
|---|---|
| -a | Data directory on remote server where AuditMaster amserver file resides. Optional if amserver resides on the same machine as the client. |
| -d | Path name of database schema (.ddf files) to import |
| -m | Master password if database is secure |
| -p | Name of application in the Product Name field in Audit Configuration window. With spaces, use quotation marks. |
| -o | Path and file name of output (.sql) file for generated SQL. If no path name is given, the file is written to the current directory. |
| -l | The default is amlog. |
| -h | Help |

The log file contains records for the current view file in AuditMaster Viewer. You can also access audit records in archived files, but queries on the current view file must be enabled first. Follow these short procedures in the order given:

1. Creating a Virtual Database
2. Running a Query on the Current View File
3. Running a Query on an Archived File

## *Creating a Virtual Database*

This section gives the steps for using the qdmg utility to create a virtual database for direct queries of audit data. The example uses the Demodata database installed with Pervasive PSQL.

1. Before setting up a virtual database, import the schema for your audited database into AuditMaster. If this already has been done, go to the next step.

   In this example, importing has already been done for Demodata as part of the AuditMaster installation.

   If you need instructions to import the schema from your own database, see the section "Managing Schemas" in Chapter 4: "Working with Audit Configurations" of *Pervasive AuditMaster User's Guide*.

2. Creation of the virtual database will require access to the DDFs of the database for which you want to query audit records. To find this path, do the following:

   a. Open Pervasive PSQL Control Center and expand the branch for the database being audited, Demodata.

   b. Open the Tables branch for Demodata, right-click on a table, and select Properties.

   c. Note the Dictionary Path where the DDFs are located. In this example, it's C:\<*installation directory*>\Demodata.

3. For the virtual database to link to audit records, you must indicate which audit configuration in AuditMaster will be used. To check its name, do the following:

   a. Open AuditMaster Viewer and log in as an AuditMaster administrator.

   b. Select Admin ▸ Audit Configuration and in the window that appears, find the product name in the list of configurations on the left. The product name is the name you entered when you imported the schema into AuditMaster. In this example, the product name is "Pervasive PSQL Demo," which was already imported when AuditMaster was installed.

4. In Windows Explorer, create a new folder at the same level as the existing Demodata folder.

In this example, we name the folder DemodataV, adding the V for "virtual," but you can choose your own name. The script to populate the virtual database will be saved here, as well as the database itself.

**5** Now use qdmg to generate the script based on the following:

- Audited database DDF path name (default installation location C:\<*installation directory*>\Demodata)
- No password, since Demodata database security is disabled.
- Audit configuration product name "Pervasive PSQL Demo"
- Path and file name for output of the generated script.

The command looks like this:

```
qdmg -d C:\<installation directory>\Demodata -p
"Pervasive PSQL Demo" -o C:\<installation
directory>\DemodataV\script
```

**6** Open a command prompt window and run the command.

The prompt returns the following message:

```
Query Data-Model Generator Utility for Pervasive
AuditMaster
Copyright (C) Pervasive Software Inc. 2004

Query Data-Model was generated into C:\<installation
directory>\DemodataV\script.sql
```

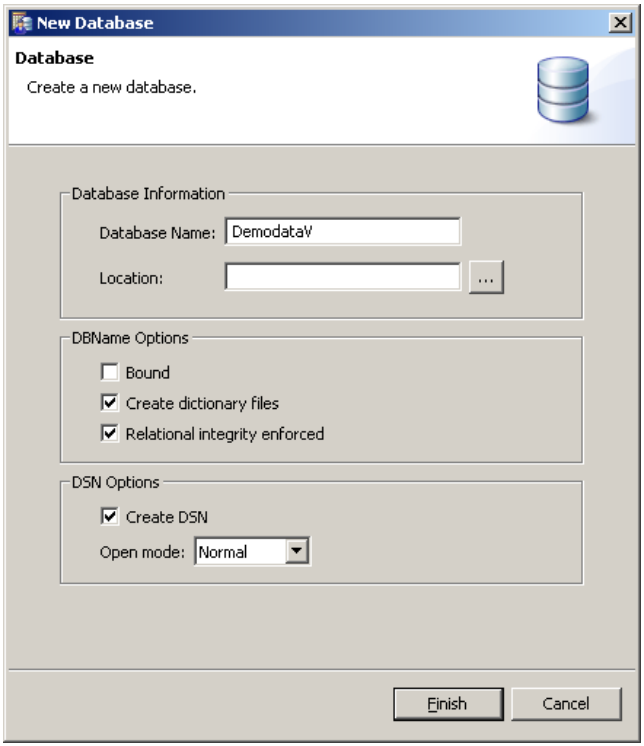
Next, create the database in which to run the script.

**7** Open Pervasive PSQL Control Center.

**8** Under the name of your server, right-click the Databases (Engine) node and select New Database.

The Create Database Wizard appears.

**9** This example uses the database name DemodataV and the directory you created, C:\<*installation directory*>\DemodataV, as shown here.




**Note** You must place the virtual database on the same volume as the AuditMaster installation directory.

**10** Click Finish to complete database creation.

**11** In Pervasive PSQL Control Center, select File ▸ Open.

**12** In the Open dialog box, navigate to the file script.sql saved earlier in C:\<*installation directory*>\DemodataV.

The Select Database dialog box appears.

**13** Expand the Databases tree, select DemodataV, and click OK.

SQL Editor displays the SQL statements in script.sql.

**14** Select SQL ▸ Execute All SQL Statements.

The statements in script.sql populate DemodataV with views to audit records.

The virtual database DemodataV now supports queries on audit record columns, as well as on data columns from Demodata.

You may now do any of the following:

- Find out what you can query. See The Structure of an Audit Record.
- Query current audit records. See Running a Query on the Current View File.
- Query archived audit records. See Running a Query on an Archived File.
- Create a delta alert. See Using the Delta Alert Utility.

## The Structure of an Audit Record

The columns of an audit record are described in this section. Its structure is representative of the result returned by a query such as `SELECT * FROM vstudent`.

The following facts should be noted in the example:

- Audit columns in the result have the prefix AM$ and contain audit data.
- After the AM$ audit data columns, the rest of the row consists of data fields from the audited table and contain values captured from that table at the time of the audit event.
- Many audit columns match query attributes seen in AuditMaster Viewer and in the Query Builder window tabs.
- All column names are queryable, but some contain internally used codes that are not particularly relevant to human auditing.

Once you have reviewed the audit record structure, see Running a Query on the Current View File for steps to run a query on the DemodataV example.

The following table compares the columns of an audit record with those displayed in the AuditMaster Viewer grid.

*Table B-1 Audit Record Columns in a Virtual Database versus AuditMaster Viewer*

| Virtual Database | AuditMaster Viewer | Description |
|---|---|---|
| AM$rec_id | Record No. | Incremental number for audit record |
| AM$opdate | Date | Capture date for audit record (e.g., 2005-06-07) |
| AM$optime | Time | Capture time for audit record (e.g., 17:04:30) |
| AM$dbms_id | — | Internal use |
| AM$dbmsverkey | — | Version of Pervasive PSQL system |
| AM$opcontextkey | Operation Context | Normal operation (e.g., BTRIEVE) or error |
| AM$opcode | — | Internal use |
| AM$optext | Operation | Database event. Events can include any item in Operations list of the Did What tab in Query Builder.<br>SQL logins display in this column. Selected Pervasive PSQL status codes also appear here when first selected in the Errors to Audit section of the Server Settings window. |
| AM$dep_rec_id | Dependent Record | Record number for an earlier related record:<br>• Modify-before record for modify-after record<br>• Begin-transaction record for end/abort transaction record |
| AM$prod_id | — | Internal use |
| AM$prodverkey | Product Version | As listed in audit configuration for monitored files |
| AM$product_name | Product | As listed in audit configuration for monitored files |
| AM$comp_id | Database Engine | Either AM Message API (internal use within AuditMaster) or Pervasive PSQL |
| AM$compverkey | Component Version | Component version, as listed in audit configuration for monitored files |
| AM$comp_name | Component | As listed in audit configuration for monitored files |
| AM$tab_id | — | Internal use |
| AM$tabverkey | — | Same as AM$compverkey |
| AM$table_name | Table Name | File in which event occurred. Same as Tables attribute under Did What tab. The file must be selected for monitoring in an audit configuration. All configured files appear in the Tables list of the Did What tab in Query Builder. |
| AM$tabdef_id | — | Internal use |

*Table B-1 Audit Record Columns in a Virtual Database versus AuditMaster Viewer*

| Virtual Database | AuditMaster Viewer | Description |
|---|---|---|
| AM$group_name | Group Name | Group for monitored files in audit configuration. Same as Groups attribute under Did What tab. |
| AM$net_id | Network Address | Same as Network Address attribute under From Where tab. One of the following:<br>• MAC ID if event in audited file originated on same system as AuditMaster server<br>• IP address for local client applications using UNC address instead of simple path name<br>• IP address if event originated from remote client |
| AM$net_user_id | User Name | Login ID under which event occurred. Same as user name under Who tab. See “Displaying Audit Records under Pervasive PSQL Security” in *Pervasive AuditMaster User’s Guide*. |
| AM$process_name | Process Name | Process that was source of audit event. Same as Process attribute under How tab. |
| AM$sess_num | — | Internal use |
| AM$lic_num | — | Internal use |
| AM$mapstate | — | Internal use |
| AM$database_name | Database Name | Database in which audit event occurred. Depending on the implementation of the database concept at the level of the event, this value may be “n/a,” not available. |
| AM$osverkey | OS Version | Name and version of operating system of machine where AuditMaster server is running (e.g., W2K 5.1.2600 SP3.0) |
| AM$retcode | — | Internal use |
| AM$reserved | — | Internal use |
| AM$databufsize | — | Internal use |
| AM$len | — | Internal use |
| <Data Column 1> | — | First data column from table where audit event occurred |
| <Data Column 2> | — | Second data column from table where audit event occurred |
| <Data Column *n*...> | — | Additional data columns... |

## *Running a Query on the Current View File*

Before querying for audit records described under The Structure of an Audit Record, be sure to have done the following:

- Run qdmg to generate a script to populate a virtual database with views linked to audit records
- Create an empty database
- Execute the script in the database

If you've completed these tasks, you're ready to run direct queries for audit records as shown in the continuing example in this section. Steps for a simple query are given, as well as those for a more complex delta query to compare Before and After field values.

### ➢ To run a simple query for DemodataV audit records

1. In AuditMaster, set the built-in Pervasive PSQL Demo audit configuration to monitor the Student table in Demodata, then restart the event handler to activate the configuration.
2. Open Pervasive PSQL Control Center, open the Demodata database, then open the Student table.

   In SQL Editor, the default query `SELECT * FROM "Student"` returns all rows.
3. The first row should contain the student ID 190907350. Click the GPA field for this student, change 4.000 to 3.000, and press Enter.
4. In Pervasive PSQL Control Center, select File ▸ New ▸ SQL Document.
5. When asked to select a database, click DemodataV.
6. In the new SQL document, run the following query. You may copy this statement and paste it in SQL Editor.

```
SELECT AM$rec_id, AM$opdate, AM$optext, ID,
Cumulative_GPA FROM VStudent
```

The query should return a result like the following:

```
 AM$rec_id  AM$opdate AM$optext             ID Cumulative_GPA
========== ========== =============  ========= ==============
637          6/2/2005 Modify Before  190907350 4.000
638          6/2/2005 Modify After   190907350 3.000
```

### ➤ To run a delta query to compare Before and After fields

For a more complex example, you may run a delta query to compare Before and After values. The general syntax for a delta query is as follows:

```
SELECT field1, field2,...
FROM view after, view before
WHERE after.AM$rec_id = before.AM$dep_rec_id AND
after.AM$field3 <> before.AM$field3
```

This type of query will display audit records for every instance of an update to field 3. For a large set of audit records, however, such a query may return too large a result. In this example, we will limit the delta query to a specific student ID.

1. Return to SQL Editor for the DemodataV database used in the last example.
2. Run the following delta query against the Before and After fields in the audit records for the ID of the student whose GPA you changed. You may copy this statement and paste it into SQL Editor.

```
SELECT after.AM$rec_id, after.AM$opdate, after.AM$optime,
after.AM$net_user_id, before.Cumulative_GPA AS "GPA
Before", after.Cumulative_GPA AS "GPA After"
FROM "VStudent" after, "VStudent" before
WHERE after.ID = '190907350' AND after.AM$rec_id =
before.AM$dep_rec_id
AND after.Cumulative_GPA <> before.Cumulative_GPA;
```

The query should return a result like the following:

```
AM$rec_id  AM$opdate  AM$optime   AM$net_user_id  GPA Before  GPA After
=========  ========== ==========  ==============  ==========  ==========
637        6/2/2005   6:23:49 PM  db_user              4.000       3.000
```

**Note** Once you're able to run a delta query against a virtual database, you can configure a delta alert. The AuditMaster delta alert feature can use changes in selected columns of an audit record as the alert condition.

## *Running a Query on an Archived File*

This section refers to the virtual database DemodataV you created under Creating a Virtual Database.

The qdmg script sets selected tables in the virtual database to point to audit records in the current view file. The default path for this file is C:\<*installation directory*>\Audit\data\amlog. As explained in this section, you can reset the path to an archived file if you know its name.

Archived file names are based on creation date, *yyyymmdd.nn*, where *yyyy* is year, *mm* is month, *dd* is day, and *nn* is number of archived file that day, starting with two zeroes. File names end in a capital V. The default folder for archived files is C:\<*installation directory*>\Audit\Arch.

When an archived file is compressed, it moves to a different folder, the default for which is C:\<*installation directory*>\Audit\Comp, and the V in the file name changes to Z. When the file is decompressed, it returns to the Arch folder and the Z changes back to V. As with queries within AuditMaster, direct queries run only on uncompressed records.

The method described in this section uses two SQL scripts:

- The first script sets the virtual database to point to an archived file instead of the current view file.
- The second script resets the virtual database to its original state so that queries again return results from the current view file.

The following steps demonstrate these scripts using the virtual database DemodataV created earlier. The examples are intended to illustrate how you can write your own versions of these scripts.

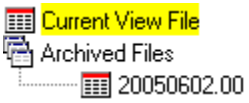
### ➢ To reset the virtual database for an archived file query

1. To use these steps, you need an archived file. Open AuditMaster, right-click the Current View File, and select Archive.

   AuditMaster moves current audit records to an archived file.

2. Double-click the Archived Files node to open it, then right-click the node and select Refresh All.

   The newly created archived file appears in the list.




3. Note the name of the file, which in this example is 20050602.00V. If you wish to see that the V is in the file name suffix, look in the archive folder, (e.g., C:\<*installation directory*>\Audit\Arch).
4. In Pervasive PSQL Control Center, select File ▸ SQL Document.
5. When asked to select a database, click DemodataV.
6. In the new SQL document, run all of the following SQL statements. You may copy and paste them in SQL Editor. Use the name of your own archived file instead of 20050602.00V.

```
-- This script resets the virtual database to
-- the uncompressed archived file 20050602.00V.
ALTER TABLE AM$amlog IN DICTIONARY USING
'\<installation
directory>\Audit\Arch\20050602.00V';
ALTER TABLE Billing IN DICTIONARY USING
'\<installation
directory>\Audit\Arch\20050602.00V';
ALTER TABLE Class IN DICTIONARY USING '\<installation
directory>\Audit\Arch\20050602.00V';
ALTER TABLE Course IN DICTIONARY USING
'\<installation
directory>\Audit\Arch\20050602.00V';
ALTER TABLE Department IN DICTIONARY USING
'\<installation
directory>\Audit\Arch\20050602.00V';
ALTER TABLE Enrolls IN DICTIONARY USING
'\<installation
directory>\Audit\Arch\20050602.00V';
ALTER TABLE Faculty IN DICTIONARY USING
'\<installation
directory>\Audit\Arch\20050602.00V';
ALTER TABLE Person IN DICTIONARY USING
'\<installation
directory>\Audit\Arch\20050602.00V';
ALTER TABLE Room IN DICTIONARY USING '\<installation
directory>\Audit\Arch\20050602.00V';
ALTER TABLE Student IN DICTIONARY USING
'\<installation
directory>\Audit\Arch\20050602.00V';
ALTER TABLE Tuition IN DICTIONARY USING
'\<installation
directory>\Audit\Arch\20050602.00V';
```

**Note** The script alters the table location property for AM$amlog in the virtual database and also for all of its copies of the data tables found in the audited database. When you write your own version of this script, be sure you do not alter the table location property for the following virtual database tables: AM$Components, AM$OpList, AM$Products, AM$Tables.

**7** After the script runs, you may want to select File ▸ Save SQL Query As to keep it for reuse, perhaps under a name such as 20050602.00V.sql.

The delta query you ran under section Running a Query on the Current View File should now return the same result as when you ran it against the current view, since those audit records have been moved into the archived file to which the virtual database now points.

### ➤ To reset the virtual database for a current view query

These steps let you run direct queries on the current view file again.

**1** In Pervasive PSQL Control Center, select File ▸ SQL Document.

**2** When asked to select a database, click DemodataV.

**3** In the new SQL document, run all of the following SQL statements. You may copy and paste them in SQL Editor.

```
-- This script resets the virtual database to the current
-- view file. For AuditMaster 6.0 or 6.1, use amview
-- instead of amlog.

   ALTER TABLE AM$amlog IN DICTIONARY USING
   '\<installation directory>\Audit\DATA\amlog';
   ALTER TABLE Billing IN DICTIONARY USING
   '\<installation directory>\Audit\DATA\amlog';
   ALTER TABLE Class IN DICTIONARY USING '\<installation
   directory>\Audit\DATA\amlog';
   ALTER TABLE Course IN DICTIONARY USING
   '\<installation directory>\Audit\DATA\amlog';
   ALTER TABLE Department IN DICTIONARY USING
   '\<installation directory>\Audit\DATA\amlog';
   ALTER TABLE Enrolls IN DICTIONARY USING
   '\<installation directory>\Audit\DATA\amlog';
   ALTER TABLE Faculty IN DICTIONARY USING
```

```
'\<installation directory>\Audit\DATA\amlog';
ALTER TABLE Person IN DICTIONARY USING
'\<installation directory>\Audit\DATA\amlog';
ALTER TABLE Room IN DICTIONARY USING '\<installation
directory>\Audit\DATA\amlog';
ALTER TABLE Student IN DICTIONARY USING
'\<installation directory>\Audit\DATA\amlog';
ALTER TABLE Tuition IN DICTIONARY USING
'\<installation directory>\Audit\DATA\amlog';
```

**Note** The script alters the table location property for AM$amlog in the virtual database and also for all of its copies of the data tables found in the audited database. When you write your own version of this script, be sure you do not alter the table location property for the following virtual database tables: AM$Components, AM$OpList, AM$Products, AM$Tables.

4 After the script runs, you may want to select File ▸ Save As to keep it for reuse, perhaps under a name such as currentview.sql.

The delta query you ran under section Running a Query on the Current View File will now return a result for the current view instead of for the archived file.

## *Summary of Direct Query Methods*

This section summarizes the direct query method for audit records:

1 A virtual database can enable direct queries of audit records independently of AuditMaster Viewer.

2 A special script populates the database. Use the Query Data-Model Generator utility qdmg to automate the writing of this script.

3 Create a database on the same volume as the AuditMaster installation root (e.g., default C:\<*installation directory*>\Audit).

4 Run the qdmg script in the database.

5 You may now run queries in the virtual database to return audit records from the current view file.

6 To enable queries of audit records in an archived file, use an ALTER script to reset the virtual database to do so.

7. Use a second ALTER script to set the virtual database back to its original state to query the current view file again.
8. Create and save a reset script for the current view file and for each archived file against which you want to run direct queries. In the virtual database, run the script you need before running your direct queries.
9. Remember that archived files must be uncompressed for queries to succeed.

## Using the Delta Alert Utility

The AuditMaster delta alerts feature provides a means of setting an email alert based on a change to a selected audit record column or columns as the monitored event. Delta alert configuration has the following steps:

1. In AuditMaster, configure one or more tables to be monitored for changes.
2. Use the qdmg utility to create a virtual database for the database of the tables you're monitoring so that you can run delta queries against captured audit records to find the alert condition.
3. Create an AuditMaster alert and enter amda.exe as the RunProgram action and set its parameters.
4. Within the alert, build a query for the Modify After event for the table or tables where the alert condition will occur.
5. Select email recipients to be notified when the alert triggers.

The details of these steps are given under Delta Alert Example, which shows how to create a working sample of a delta alert on the Demodata database.

## *Parameters for the amda Utility*

The parameters for the amda utility define the test for the delta alert.

`amda -d` *database* `-t` *table* `-r @RecID -c` *columns* [`-u` *username*] [`-p` *password*] [`-o` *operator*]

### *Parameters*

| Option | Description |
|---|---|
| -d | DSN of the virtual database created using QDMG |
| -t | Name of table to query |
| -r | Placeholder parameter '@RecID' for the record ID of the required row in the queried table |
| -c | Name of one or more columns to test, comma-separated with no spaces |
| -u | User name if database security is enabled |
| -p | Password if database security is enabled |
| -o | Boolean operator 'or' (default) or 'and' when querying more than one column |
| -h | Help |

For example, the following entry as a RunProgram alert action tests audit records for events marking changes in either the column for amount owed or the column for amount paid in the Billing table in Demodata.

```
amda -d DemodataV -t Billing -r @RecID -c
Amount_Owed,Amount_Paid
```

This same delta alert is used under Delta Alert Example.

## Setting Delta Alert Email Recipients

The file amdaemail.cfg is used to set the mail server, domain, and recipients of email alerts sent by AuditMaster when delta query conditions are true. In a default installation, the file is found in C:\<*installation directory*>\Audit\Data. It contains the following text:

```
; ************************************
; *  Delta Alert Email Configuration  *
; ************************************

; This is a comment.
[SMTP INFO]
;<SMTP Server>
;<Domain>

[EMAIL INFO]
;<email address1>
;<email address2>
;<.............>
```

The commented variables enclosed in angle brackets are replaced with the values needed for the delta alert to notify mail recipients.

The values in a configured amdaemail.cfg file will look like the following:

```
[SMTP INFO]
smtp-server
company.com

[EMAIL INFO]
user.name@company.com
```

## *Delta Alert Example*

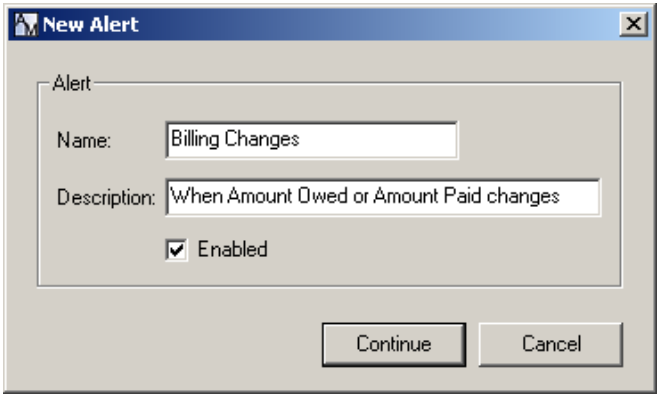
This section provides steps to create and configure a delta query to alert recipients by email when billing amounts are changed in the Demodata database.

### ➤ To set up a delta alert

1. In AuditMaster, be sure the table or tables to be monitored have been added to an audit configuration. In this example, the table is Billing in Demodata.
2. Follow the instructions under Creating a Virtual Database.

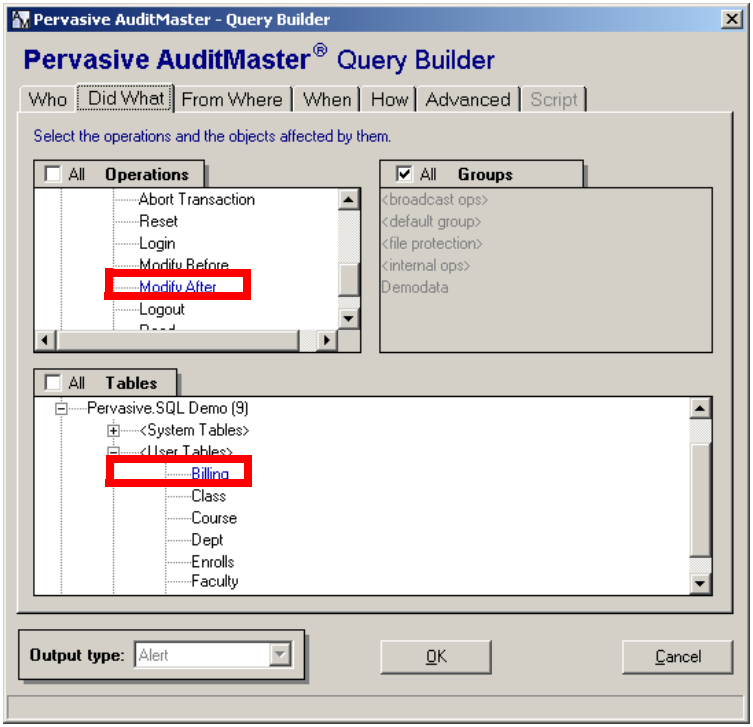
   You must use the qdmg utility on the monitored database to enable the delta alert feature to run. This example uses Demodata.

   If you've already created DemodataV, go to the next step.
3. In AuditMaster, using the steps given under Working with Alerts, create the following alert:




4. In the query for Operations, under Pervasive PSQL(Btrieve) select Modify After.
5. For Tables, under User Tables select Billing.

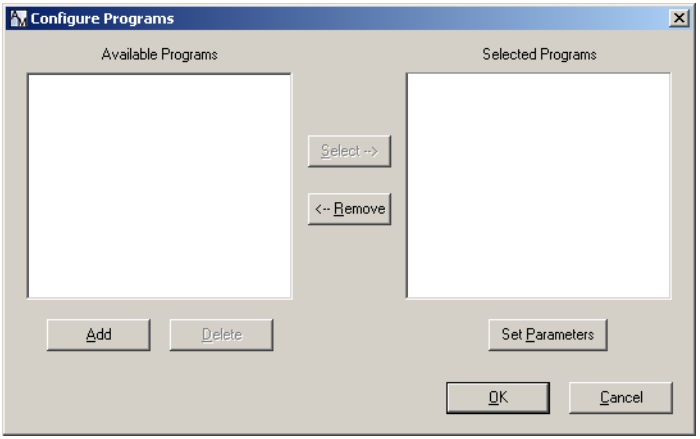
   Query Builder should now look like the following:




**6** In the Action for Alert dialog box, select RunProgram.

**7** To configure RunProgram, add and select amda.exe, which is found in a default installation in C:\<*installation directory*>\Audit\bin\.

The Configure Programs dialog box will look like the following:

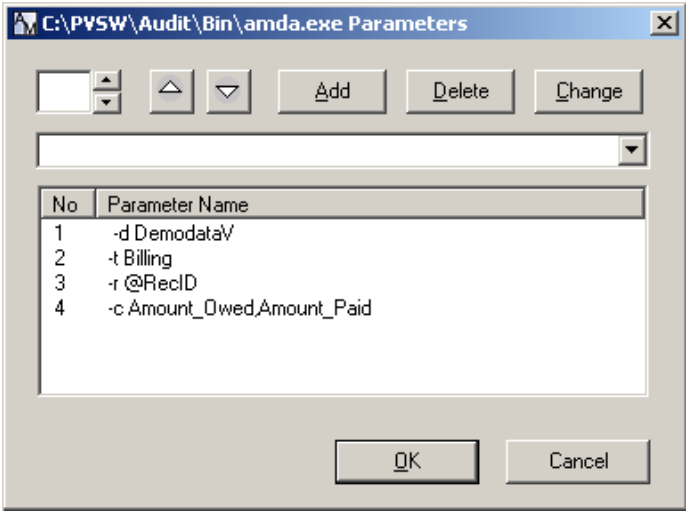



**8** To store the amda command parameters, click Set Parameters and make entries based on the following:

```
amda -d DemodataV -t Billing -r @RecID -c
Amount_Owed,Amount_Paid
```

For information on this step, see Setting a RunProgram Action and Parameters for the amda Utility.

The entries will look like the following:




**9** Set email recipients in amdaemail.cfg. For information on this step, see Setting Delta Alert Email Recipients.

10 Close AuditMaster Viewer and restart Pervasive services to activate the delta alert.

11 In Pervasive PSQL Control Center, open the Billing table in Demodata and change a value in the Amount_Paid column.

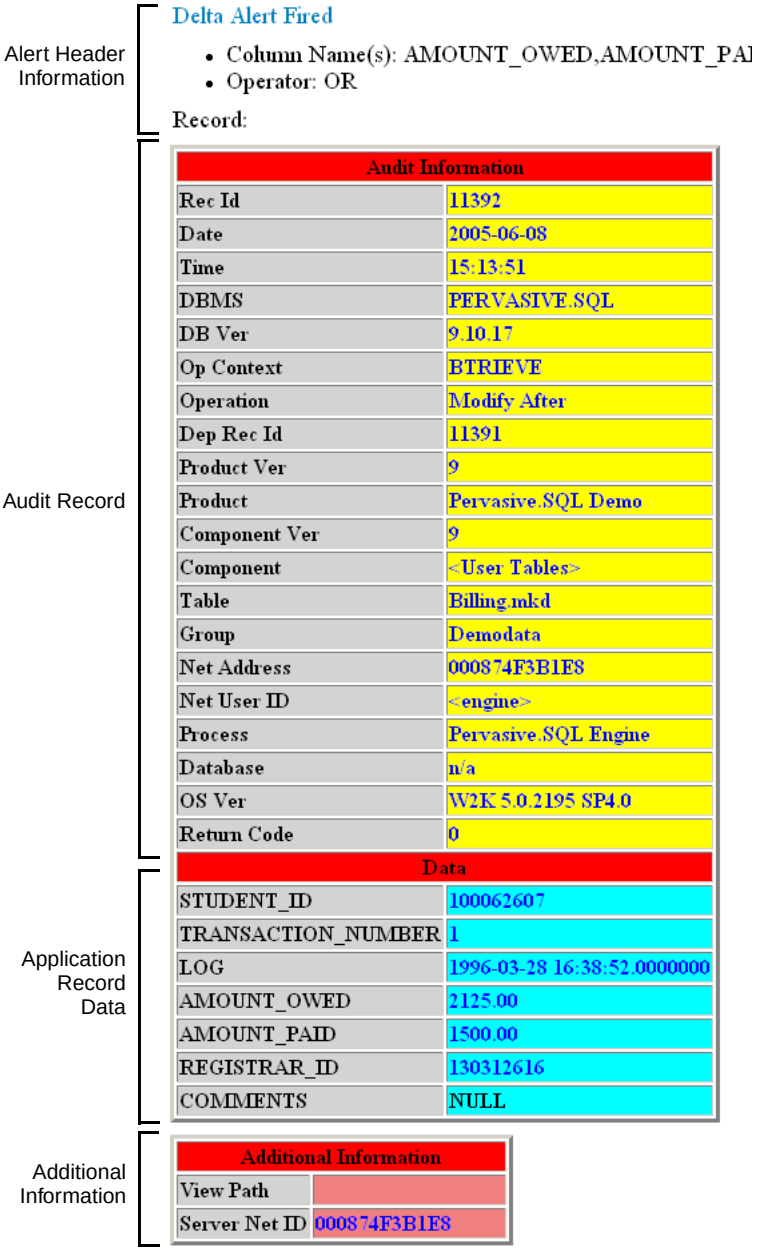
   A command prompt window announces that column values have changed and email is being sent to recipients.

Recipients receive a message with a header like the following:

From: Auditmaster
Sent: Wednesday, June 08, 2005 3:14 PM
To: DeltaAlertRecipients
Subject: Delta Alert Fired on Record ID 11392

Record ID is the number of the audit record that triggered the alert. The body of this sample mail message looks like this:

*Figure B-1 Structure of a Delta Alert Email Message*



# *Index*

## Numerics

-108 error message 8-3

## A

Actions
  setting EmailAlert 7-30
  setting for an alert 7-28
  setting RunProgram 7-34
  stopping by deleting alert 7-37
  stopping by disabling 7-37
Administrator
  AuditMaster, defined 4-3
Advanced query tab
  Select Type attribute
    case sensitive 7-19
Advanced tab 7-16
  restricting queries at the column level 7-18
Alerts 7-25
  adding a new alert 7-25
  deleting to stop 7-37
  editing 7-36
  setting an action for 7-28
  working with 7-24
amda
  parameters B-23
amdaemail.cfg file B-24
AMMON paths, changing 8-22
AMMON settings, changing 8-22
amserver file, described 8-2
Archived files
  grayed out in data tree 7-8
  setting number to show in data tree 7-10
Archiving
  automated in server settings 8-23
Audit configuration
  making changes to an existing 6-7
Audit record
  numbering limit A-2
Audit record grid 7-4
  effect of security policy on names 7-44
audit record grid
  customizing 7-5
Audit records
  displaying 7-2
  exporting to another application 7-43
  querying through SQL B-7
  searching 7-40
  sorting 7-42
  viewing details 7-7
Audited operations
  Pervasive PSQL status codes 7-6
  SQL logins 7-6
AuditMaster
  administrator, defined 4-3
  description 1-2
  documentation 2-3
  features 1-3
  installing 3-1
    checklists 2-4
    client only 3-6
    common questions after 3-10
    hardware requirements 2-5
    how to uninstall 3-11
    permission required 2-5
    under Windows 3-4
  product components 2-2
  readme file 2-6
  uninstalling 3-11
  utilities 2-2
Authorization License 2-5

## B

Before and After columns, defined 7-7

## C

Checklists for installing AuditMaster 2-4
Columns
  Before and After 7-7
  changing order in audit record grid 7-5
  changing which are visible in audit record grid 7-5

Comma-delimited file, creating from audit data 7-43
Common settings, changing 8-22
Components
log event handler 1-4
viewer 1-4
Configuration conflicts
resolving 6-27

## D

Data definitions
configuring with 6-9
Data tree, defined 5-2
Database names
effect of security policy on 7-44
Delta alerts
amda parameters B-23
email message example B-29
example B-25
overview B-22
setting mail recipients B-24
Detail view
audit records
description 7-7
Did What query tab, using 7-14
Disk full
opening the status log viewer when 8-16
restarting the status log after A-4
Documentation for AuditMaster 2-3

## E

EmailAlert action, setting 7-30
Error message
-108 8-3
Export tool, using 7-43

## F

Features 1-3
Files tab
using in queries 7-21

## G

General tips
audit record numbering A-2
configuring audited files on the same machine as AuditMaster server A-2
Pervasive PSQL optimization A-2

## H

Hardware required to install AuditMaster 2-5
How query tab, using 7-14

## I

Importing
schemas 6-18
Installation of AuditMaster
See AuditMaster, installing

## K

Keys, changing 8-22

## L

Last query executed, running 7-22
License, authorization 2-5
Log event handler
description 1-4

## M

MAC or IP address displayed in audit record 7-6
Menus
shortcut 4-12
Monitoring
Pervasive PSQL status codes 7-6
SQL logins 7-6

## N

Network communications
testing A-7
Network share
removing 8-6
Numbering
audit record limit A-2

## P

Permissions
required to install AuditMaster 2-5
Pervasive PSQL status codes
as audited operations 7-6
Pervasive PSQL utilities. *See* Utilities.
Pervasive Software

Website A-9
Printing reports 7-38
Product components of AuditMaster 2-2
Prompt for Client Credentials
setting to run AuditMaster in a secure database 3-3, 4-6

## Q

Queries
building advanced 7-16
displaying all audit records (query for everything) 7-14
restricting 7-14
restricting at the column level in Advanced tab 7-18
Query Builder
description 7-13
window 7-13

## R

Readme file 2-6
Release notes 2-6
Reports, printing 7-38
Resources, additional iv-xii
RunProgram action
setting 7-34

## S

Saved query, running 7-22
Schemas
configuring without 6-2
importing 6-18
Search tool, using 7-40
Security policy
effect on names in audit record grid 7-44
Server description
editing 8-5
Server keys
maintaining 8-22
Server Settings
Automated Archiving section 8-23
Servers
adding 8-2
and the amserver file 8-2
defined 5-2
removing 8-5
renaming. *See* Server description
editing 8-5
Shortcut menus, using 4-12
Sort tool, using 7-42
SQL
querying audit records directly B-7
SQL logins
as audited operations 7-6
Status code 94
after changing database security policy 4-10
Status codes
Pervasive PSQL
auditing 7-6
Status log records
filtering 8-16
sorting 8-16
viewing 8-16

## T

Tab-delimited file, creating from audit data 7-43
Testing
network connectivity A-7
Tips
application data A-2
Pervasive PSQL A-2
Toolbar, using icons from 5-4
Troubleshooting
network connectivity A-7
strategies A-3

## U

Undo 7-45
Uninstalling AuditMaster 3-11
User maintenance 8-18
User names
effect of security policy on 7-44
User, defined 4-3
Users
adding or removing 8-18
changing user type 8-18
Utilities
AuditMaster 2-2
overview 6-1, 7-1

## V

View file
    defined 5-2
Viewer
    description 1-4

## W

Web sites
    Pervasive Software A-9
When query tab, using 7-14
Where query tab, using 7-14
Who query tab, using 7-14